CSI adhyayan

April - June 2016

Celebrating Golden Jubilee

Discovering the Potential

Computer Society of India

A National Publication Dedicated to IT Education, Research and Student Community

www.csi-india.org

ABOUT CSI

The seed for the Computer Society of India (CSI) was first shown in the year 1965 with a handful of IT enthusiasts who were a computer user group and felt the need to organize their activities. They also wanted to share their knowledge and exchange ideas on what they felt was a fast emerging sector. Today the CSI takes pride in being the largest and most professionally managed association of and for IT professionals in India. The purposes of the Society are scientific and educational directed towards the advancement of the theory and practice of computer science and IT. The organisation has grown to an enviable size of 100,000 strong members consisting of professionals with varied backgrounds including Software developers, Scientists, Academicians, Project Managers, CIO's , CTO's & IT vendors to just name a few. It has spread its branches all over the country. Currently having more than 500 student branches and rooted firmly at 73 different locations, CSI has plans of opening many more chapters & activity centres in smaller towns and cities of the country. The idea is to spread the knowledge, and provide opportunities to as many interested as possible.

The CSI Vision: "IT for Masses"

Keeping in mind the interest of the IT professionals & computer users CSI works towards making the profession an area of choice amongst all sections of the society. The promotion of Information Technology as a profession is the top priority of CSI today. To fulfill this objective, the CSI regularly organizes conferences, conventions, lectures, projects, awards. And at the same time it also ensures that regular training and skill updating are organized for the IT professionals. Education Directorate, CSI helps physically challenged citizens by providing training 'Punarjani'. CSI also works towards a global approach, by seeking out alliances with organizations overseas who may be willing to come forward and participate in such activities. CSI also helps governments in formulating IT strategy & planning.

Contents

Big Data and Veracity Challenges	5
A Day in A World Run by the IoT	8
A Survey of Cryptographic Techniques And Applications	12
Blue Eye Technology	35
Cloud Computing	38
Cyber Forensics	41
FLS: Signal Generation For Congestion Detection And Prevention In Adaptive Networks	43
Gesture Based Audio/Video Player	49
Green Computing	55
Green Technology	60
Humanoid Robot	63
Connecting India Through Li-Fi Technology	65
Fire Detection Through Image Analysis	68
Travelyan :Travel Buddy	77
Attendance Monitoring	82
The Deep Web: Let's Dive	89
Top10 Tools For Natural Language Processing -Research And Development	92
Underwater Sensor Network	97
Virtual Reality And Its Applications	99
Virtual Reality	105
Firewall	110
Sixth Sense Technology	113
Basic of Networking	116
Wireless Charging of Mobile Phones Using Microwaves	120
ihome Automation: A Better Way for Home Automation	126

Disclaimer: CSI Adhyayan contains information about new technologies useful for students. The information contained in this newsletter is not advice, and should not be treated as such. You must not rely on the information in the newsletter as an alternative to information from research journals.

We do not represent, warrant, undertake or guarantee:

- that the information in the newsletter is original, correct, accurate, complete or non-misleading
- that the use of guidance in the newsletter will lead to any particular outcome or result; or We will not be liable to you in respect of any losses arising out of any event or events beyond our reasonable control. We will not be liable to you in respect of any business losses, including without limitation loss of or damage to profits, income, revenue, use, production, anticipated savings, business, contracts, commercial opportunities or goodwill. We will not be liable to you in respect of any loss or corruption of any data, database or software. We will not be liable to you in respect of any special, indirect or consequential loss or damage.

BIG DATA AND VERACITY CHALLENGES

Compiled by:

Greeshma K Babu and Sajna Francis

ABSTRACT

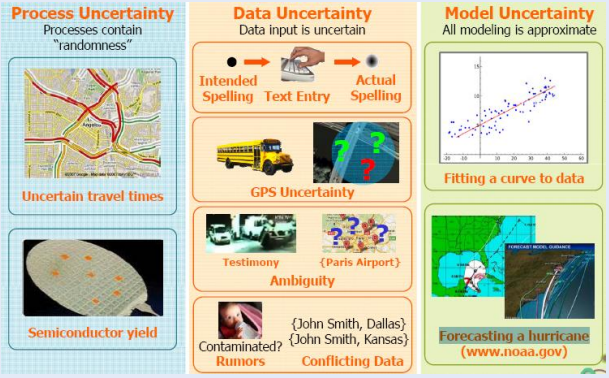
This paper points out that big data consist of different characteristics which affects its quality. The term big data is defining a collection of large and complex data sets that are difficult to process using conventional data processing tools. Every day, we create billions of data all over the world. These data comes from scientific experiments, social networking sites, sensor networks, mobile conversations and various other sources. Big data divided into many dimensions: Volume, Velocity and Variety. To improve the quality of this three dimension a new dimension veracity was introduced. This paper provides an analysis about the concept of veracity. Veracity can be explored mainly based on three dimension objectivity/subjectivity, truthfulness/deception, credibility/implausibility. These dimensions are combined to form one composite index- the big data veracity index. This index is useful for assessing systematic variations in big data quality. The paper contributes to the big data research by dividing the existing tools to measure the suggested dimensions.

INTRODUCTION

"Without big data analytics, companies are blind and deaf, wandering out onto the web like deer on a freeway." – Geoffrey Moore

Big data is used in organization for storing ,managing ,and manipulating vast amounts of Disparate data at right speed at right time. To Achieve the right uses the big data can be divided based on three characteristics like volume, velocity, variety. Big data is a large or complex set of data in which cannot be managed by traditional data processing applications. The major challenges involved include analyzing , capturing, searching, sharing, storing, transferring, visualizing, queering and privacy of information. This term refers the using of predictive analysis and seldom to a particular size of data set. Big data accuracy may helps in decision making, and better decisions lead to greater efficiencies in operations, reduction in cost and it also reduces the risk [1] .The three dimensions of big data: volume-amount of data. Variety-data in various forms .velocity-how fast data is processed. Veracity is the fourth dimension. The biases, noise and abnormality in data can be referred to as big data veracity. Compared to velocity and volume veracity is a biggest challenge. The data should be clean so that 'dirty data' will not accumulate in your systems. [3]. If the data is inaccurate, is unreliable, the organization may face a big problem, especially the organization for selling information like the marketing ones. Due to the volume of information the veracity is the hardest thing to achieve with big data. The three dimensions of veracity include: objectively, Truthfulness, credibility. These dimensions may cause errors and decrease in big data quality. The Veracity issues arise due to:

1. Process Uncertainty (Processes contain randomness) Example _Uncertain travel times, Semiconductor yield 2.DataUncertainty (Data input is uncertain) Example _GPS uncertainty, Ambiguity, Conflicting Data, Model Uncertainty (All modeling is approximate) Example- Fitting a curve to data, forecasting a hurricane.



CHALLENGES:

- How perfect is the sampling resolution?
- How can we manage the uncertainty, imprecision, missing values, and misstatements?
- Checks whether the data is good?
- Is the reading on time?
- Are the sampling biases understandable?
- Checks whether data is available to all?

Web has significant practical importance as online rumor and misinformation can have tremendous impacts on our society and everyday life. One of the fundamental difficulties is that data can be biased on noisy, outdated, incorrect, misleading and thus unreliable. Conflicting data from multiple sources amplifies this problem and veracity of data has to be estimated. Beyond the emerging field of computational journalism and the success of online fact-checker (e.g., Fact Checks, Claim bus)truth discovery is a long-standing and challenging problem studied by many research communities in artificial intelligence, databases, and complex systems and under various names: fact-checking, data or knowledge fusion, information trustworthiness, credibility or information corroboration for a survey and for a comparative analysis. The ultimate goal is to predict the truth label of a set of assertions claimed by multiple sources and to infer sources' reliability with no or few prior knowledge. One major line of previous work aimed at iteratively computing and updating the source's trustworthiness as a belief function in its claims, and then the belief score of each claim as a function of its sources' trust-worthiness. More complex models have then included various aspects other than trustworthiness of source and claims belief such as the dependence between sources the correlation of claims, the notion of evolving truth [5].

CONCLUSION

In this paper we points out that big data is a collection of large and complex data set that is difficult to manage using database management tool. Management tool includes processes data like capture, storage, visualization search, sharing and analysis .*In* 2001, the dimension also called as 3v model were introduced .The 3vs were not enough for storing big data. So a new dimension called Veracity was introduced .Uncertainty of big data directly affect veracity .Challenges are always a threat to veracity that include: How the major challenges like lack of certainty can be solved. Checks whether the data is good? How large is the coverage? How perfect is the sampling resolution? Are the readings on time? Are the sampling biases understandable? Checks whether data is available to all? So, we conclude that veracity is a new dimension that is used for maintaining a balanced form of big data.

REFERENCE

1. Cronin, Blasé (2013). Editorial. *Journal of the American Society for Inform. Science & Technology, 63*(3), 435–6.
2. http://insidebigdata.com/2013/09/12/beyond-volume-variety-velocity-issue-big-data-veracity/
3. “Big Data for Good”, Roger Barca, Laura Haas, Alon Halevy, Paul Miller,Roberto V. Zicari. *ODBMS Industry Watch*, June 5, 2012.
4. http://perso.telecomparistech.fr/~ba/publications/laurechallenges2015.pdf

About the Authors:

Ms. Sajna Francis

sajnafrancis@gmail.com

CSI ID NO: 01295346

Ms. Greeshma k babu

greeshmababu121@gmail.com

CSI ID NO: 01295331

Guided by:

Mr. Hari Narayanan A.G

Asst. Prof of Computer Science Department

Amrita School of Arts and Science, Kochi

Amrita Vishwa Vidhyapeetham

A DAY IN A WORLD RUN BY THE IOT

Compiled by:

Zaid Merchant

"...Therefore, we may consequently state that: this world is indeed a living being endowed with a soul and intelligence… a single visible living entity containing all other living entities, which, by their nature, are all related."

--Plato, Timaeus, 4th Century B.C.

In all of twenty-five centuries till date, there couldn't have possibly been a more appropriate way to describe the Internet of Things. It's been dubbed as "The Next Big Thing", "The Future", "The Biggest Game-Changer since the Internet itself". IBM has announced that Watson IoT unit's global headquarters will be in Munich, and with this, has made its largest investment in Europe in over two decades - simply for growth in IoT. And of course, we've all been bombarded by tons of articles on the Internet of Things. But what is the fuss all about? How will our lives change with the advent of IoT? What will our environment be like, in such a world? How different will each day be in our life? Here's how:

The alarm rang out. Softly at first, and then growing louder with every passing second. His watch began vibrating, and John woke up. He didn't groan. He knew his alarm had calculated the time it would take for John to reach his office, based on the real-time traffic scenario en route, and given him the maximum time to sleep. In his world, the concept of "I wish I had slept more/less" did not exist.

John Smith lived in a smart city, the 2nd of its kind after Songdo, South Korea. This city had an intricate system of waterways as well (with rivers and a bay), and these were monitored with wireless technology by a company, which had John as one of its Team Leads.

John's watch had detected the change in the rate of pulses once John was awake. Based on this detection and output, the process of warming the water for his bath had been initiated, conserving huge quantities of energy (if seen on a large scale), just by warming the water to appropriate amounts. As he walked into his bathroom, the sensors detected the signals, based on BLE (Bluetooth Low Energy hardware) constantly given out by his watch, and the lights came on. He showered and changed, and just as he opened his room's door, the coffee machine chugged into gear, while the lights came on and went off in the room he entered and exited respectively. A smile spread across his face, as he could not help but remember the outdated notion that the IoT world was just a complicated way to sense and take readings. The truth was, objects in the IoT were not only devices with sensory capabilities, but also provided actuation capabilities, and his coffee machine was proof enough.

John sauntered over to the fridge and read the contents of the small screen on it. The screen described the health of the contents of the fridge, which the fridge itself measured smartly. Most of it looked fine, but the apple and carrots were estimated to go bad in two days' time. With a couple of touches on the same screen, he had ordered for a fresh batch of apples, which would be delivered by evening. He finished his coffee, and placing a currency note at the appropriate position

on the table near his door, he headed out. Almost immediately, he was alerted about his friend's birthday. John promptly sent a message to wish him a happy one.

John drove to work. Yes, he actually drove himself, because automated cars, though a futuristic concept, is still not a concept within the purview of the Internet of Things. He settled in for his drive to work and began thinking of the two major problems the IoT faced on its way to where it is now. The first of the two was Privacy. It was a ludicrous problem, really. The problem still existed, as some people believed that their personal lives were personal no more, because virtually all data could be collected through some means. He did not know what such people took the data handlers for. Those guys were busy people with important tasks including, but not limited to, national and international security. They analyse and scan through various audio and video feeds for potential threats. They are genuinely not interested in knowing what you think about your boss or how much you love your mother. And they most certainly do NOT laugh at and pass around a video of you tripping and falling flat on your stomach. Sure, Big Brother is watching. But only the bad guys. The potential threats.

John breezed through the electronic toll collection system, which identified his car and automatically debited his account with the required amount, without even requiring John to slow down, another magical advantage of the IoT. He started thinking about the second problem. The problem of enough identifiers for all objects in the IoT. It was estimated that by the year 2020 itself, there would be 26-30 billion objects wirelessly connected to the Internet of Things. As a result, there was a need to have unique identifiers for each object, and yet not run out of distinct identifiers. It was decided that these devices will use an IP address as a unique identifier. The format in use was the Internet Protocol version 4 (IPv4). However, due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT would have to use IPv6 to accommodate the extremely large address space required. It was due to this feature of the IPv6, that this system was able to scale to the large numbers of objects envisaged. The rest of the world's ability to shift and adapt to IPv6 would play a major and inverse role in affecting the time they would take to become "smart" as well...

His thoughts were interrupted by a car whizzing past him at a speed that was easily in excess of twice the speed limit. Sure enough, a short distance away, it triggered the speed-gun, attached to a pole. That car would now be pulled up at the next police checkpoint, which wasn't very far. You never can outpace and outsmart a smart city. Meanwhile, John took the next right and entered his office compound, which had a proper detection mechanism in place, which recognized John and his car and promptly opened up the automated gates.

John entered the control room with his partner, Frank. The two of them were Team Leads for a specific duration during the day. Their team monitored a particular region of the waterways, in case of any emergencies and the like. The waterways were previously just a chaotic path with multiple independent ferry services operating. There were security issues, rescue issues and communication issues that constructed this giant mess. The question that arose was, how do you protect a fleet of ships and thousands of passengers every year without an Internet connection? Very soon, company officials realized the answer was "you don't." As a result, each ferry was given special routers for dynamic internet access, i.e., continuous internet access, despite the ferries moving constantly. The ferries were also allotted video surveillance equipment, for real-time, high quality audio and video feed. There was also a feature that allowed the control room to speak directly to the captain of a ferry or make an announcement in one ferry, in multiple ferries, or in case of an emergency, in all the ferries, simultaneously.

It was a pretty straightforward day for John and Frank, overseeing the movement of bridges on detecting the arrival of a large ship, and handling traffic as well, all synchronized and automatically executed by this beautifully connected system. The waterways' own Internet of Things. However, an hour before they were scheduled to leave, an emergency popped up. The captain of one of the ferries contacted them, alerting them that one of the passengers aboard was having a heart attack. John zoomed in on the particular ferry's immediate surroundings, while Frank checked the live video feed to confirm the captain's message. The ferry was diverted to the nearest alighting site, while surrounding ferries told to adjust their pace accordingly to avoid a mishap. A medical boat was alerted for immediate assistance, as was an ambulance, which was present before the ferry docked in. It was smooth. It was perfect. It was only possible because of the Internet of Things.

John and Frank were soon off-duty, and headed to the tennis court for practice. En route, John's phone, synced with his doorbell, vibrated. He checked the screen, which transmitted the live feed from outside his door. It was the apples and carrots that he had ordered earlier. With a few touches, a small window had opened on the side of the door. He watched as the delivery boy put in the bag with the foodstuff through the window, then reached in and took the currency note which John had kept earlier on the table, as a tip, smiled at the camera and left. From far away, near his tennis court, John closed that window with a touch. Almost instantly, a pop-up on his phone asked for confirmation of the delivery of foodstuff. John confirmed it, and an appropriate amount of money was transferred. The Internet of Things at work again.

John and Frank played tennis for a couple of hours. Obviously, if we're talking about a world driven by the Internet of Things, it would not have been just normal tennis. The two of them used racket sensors, which monitored their stroke, power, effectiveness, and more importantly, their mistakes. Their shoe sensors tracked the distance they ran, and with effective algorithms, the two put together, gave effective graphs on their phones on how to up their game. Who needs coaches anymore when you have the Internet of Things?

After a shower, the two headed out for drinks. They both had to drive back home, hence and to be careful about the alcohol intake. Small sensors were freely available with watches, phones as well as separately, which acted as breath-analysers and detected the levels of ethyl alcohol, and displayed them on a thick line on their respective phone screens, while the line varied in colour from green to red, symbolizing the alcohol levels. The two had drinks and shared their troubles, checking the consumption levels after regular intervals. Once it touched yellow, they decided to have dinner and leave.

John was driving home, when another car sped by him. He watched it as it swayed dangerously at high speed, and disappeared into the distance. It was a few minutes later, when he saw the car. It had swerved off the road, and hit an adjacent tree. John thought about the standard procedure which was already underway. The crash had been detected by various sensors of the car, and an immediate signal had been auto-sent to the nearest ambulance station, with the victim's wristwatch sending real-time data about his pulses to the ambulance as it rushed to the spot, which it located using the GPS data that the car had sent after the crash. It was neat. It was effective. It was the Internet of Things.

John reached home tired. He wondered why the watch hadn't already informed him that he was tired and advised him to go to sleep. A glitch? It seemed unlikely. He kept the apples and carrots in the fridge, and observed keenly as the smart fridge now began to sense, note and display the health of these newly added items. He trudged to his bedroom, and the lights switched on and off in accordance to his movements among the rooms. Just as he was about to sleep, the clock struck twelve, and his alarm clock went off. He looked at it, puzzled. Seconds later, his watch was vibrating

and his phone alarm went off as well. The Internet of Things had detected an important event in his life, and was acting accordingly. He rushed to his phone, and stared at the screen in disbelief. He switched off his phone alarm, and the alarm clock and his watch went silent and stable once more as well. With shivering hands, he dialed a familiar number. It was his girlfriend's birthday, and he was going to be a full sixty seconds late in wishing her. Truly, there will always be disasters that the Internet of Things cannot save you from.

About the Author:

Mr. Soham Mehta [CSI: 01322941] is the student of D J Sanghvi College of Engineering pursuing the Bachelor of Engineering in Information Technology. Being the Chairperson of student chapter "Computer Society of India" at D J Sanghvi, he has played an active role in managing various events such as technical workshops, seminars and hackathons throughout the year across the college. His passion for learning new technologies in tandem with constant innovation drives him for being an active member of CSI.

A SURVEY OF CRYPTOGRAPHIC TECHNIQUES AND APPLICATIONS

Compiled by:

A. Anasuya Threse Innocent and Sangeeta .K

Cryptography is an art and science which provides security for the data being stored or transmitted. The cryptographic techniques have emerged from manual to modern techniques which utilize the power of computing of existing times. Classical techniques produce cipher either by substitution or transposition, while modern techniques focus on the generation of secret keys for information exchange. The increase in volume and sensitivity of data communicated and processed over the Internet has been accompanied by a corresponding demand for safeguarding communications techniques where entities can participate in a secure fashion. Due to the increasing need for secure communications, cryptography extends its application in day to day use. This paper briefly gives a survey of the cryptographic methods and applications.

INTRODUCTION

The word Cryptography is derived from two Greek words; kryptos meaning hidden or secret and graphos meaning I write or writing [Stallings, 05]. Cryptography is the art and science of secret writing or hidden writing. The basic terminologies used in cryptography [Stallings, 05] and [Menezes, 96] are; plaintext means the normal text which is the readable and understandable one. Ciphertext is the unreadable and unintelligible format derived from the plaintext by a process called encryption. Encryption is the process of converting plaintext into ciphertext with the help of a secret parameter or mathematical information called key. The reverse process of obtaining the plaintext from the ciphertext with the help of key is called as decryption. The persons those who work on cryptography or the encryption – decryption processes are called as the cryptographers. The study of methods for obtaining the meaning of encrypted information without access to the key is called as cryptanalysis or simply code breaking. The persons those who perform cryptanalysis are called as cryptanalyst. The study of characteristics of languages which have some application in cryptography, i.e., frequency of data, letter combinations, universal patterns, etc is called as Cryptolinguistics.

The history of cryptography is briefly explained in Section 2. Section 3 briefs the ciphers, Section 4 describes the hash functions and Section 5 gives an outline of various branches of cryptography. Section 6 explains the applications of cryptography, Section 7 touches the cryptanalysis part, and Section 8 concludes.

HISTORY OF CRYPTOGRAPHY

The age of cryptography is more than 4500 years. The history can be broadly classified into; ancient cryptography, medieval cryptography, cryptography from 1800 AD to World War II, and modern cryptography.

The ancient cryptography is the one before the birth of Jesus Christ, which covers the hieroglyphics from Egypt to the Caesar cipher. Medieval cryptography starts with the religiously motivated textual

analysis technique for breaking monoalphabetic ciphers by al-Kindi of Arab and expands till the Vigenere cipher. Machine ciphers played a major role during World wars. The modern cryptography begins with Claude Shannon, the father of mathematical cryptography, which involves the use of computers. Number theory is the branch of mathematics that is purely dedicated for cryptographers. The timeline of cryptography is shown in Table 1.

The timeline of cryptologic research can be broadly classified into three; manual, machine, and computer. The manual crypto involves the ancient cryptography mainly with substitution and permutation. The machine crypto involves the use of rotor machines and the computer crypto refers to the modern cryptography with the use of computers.

Table 1. Timeline of cryptography.

Sl.No.	Timeline		Application
1	Ancient Cryptography	1900BC	Non-standard hieroglyphics [Egypt]
2		1500BC	Mesopotamian pottery glazes
3		500BC	Atbash cipher [Hebrews]
4		400BC	Polybius cipher [Greek], Scytale [Spartan]
5		50BC	Caesar cipher
6	Medieval Cryptography	800 AD	Cryptanalysis [al-Kindi, Arab]
7		1467	Polyalphabetic cipher by Leon Battista Alberti – Father of Western Cryptology, Cipher disk
8		1518	Tabula recta – square table of alphabets by Jo hannes Trithemius
9		1586	Vigenere Cipher
10	Cryptography from 1800 AD to World War II	1854	Playfair cipher
11		1857	Beaufort's cipher
12		1917	Vernam one-time pads
13		1918	Enigma machine [Germany]
14		1921	Hebern machines [Great Britain]
15		1929	Hill cipher
16		1934	Hegelin machines
17	Modern	1973	Feistel networks

18	Cryptography	1976	Public key cryptography, DES
19		1979	Secret sharing
20		1982	Secure Multiparty Computation [Yao's protocol]
21		1985	Zero knowledge [Goldreich, Micali]
22		1988	Multivariate cryptography [MKPC]
23		1980 – 1990	RC5, Blowfish, IDEA etc.
24		1990	Differential cryptanalysis
25		1994	Linear cryptanalysis, DNA Computing
26		1995	Neural Cryptography
27		1997	Triple-DES
28		1998 – 2001	AES
29		2004	Commercial quantum cryptography system available from id Quantique [Geneva, Switzerland]
30		2004 onwards	Researches to develop lightweight encryption algorithms, and to intertwine compression along with security to achieve better storage and transmission efficiency
31		2006 onwards	Security in cloud computing
32		2009 – 2013	Fully homomorphic encryption; practical system HELib implemented in 2013

CIPHERS

The cryptographic techniques [Stallings, 05], [Menezes, 96] for generating ciphers can be broadly classified into two; classical and modern as depicted in Figure 1. The classical techniques are the one carried out with paper and pen which produces the simple substitution ciphers, transposition ciphers, product ciphers, and machine ciphers with the help of rotor machines. The modern techniques are carried out with computers, which have mainly two types of encryption; symmetric encryption, which produces the stream and block ciphers, the asymmetric encryption which produces only block ciphers. The substitutions and permutations with higher complexity are used in modern ciphers. Beyond this, according to [Stallings, 05], cryptographic systems can be characterized along three independent dimensions: (i) the type of operations used for encryption; which can be of substitution and/or permutation, (ii) the number of keys used; accordingly, single key/ secret key cryptography or two-key/ public key cryptography, and (iii) the way in which plaintext is processed; such as block cipher or stream cipher.

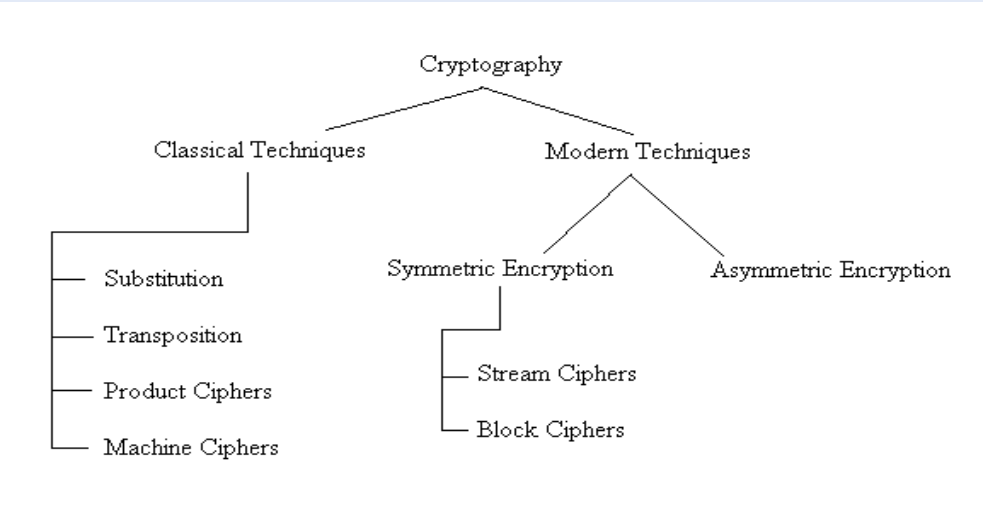


Figure 1. Classification of ciphers

CLASSICAL TECHNIQUES

Classical encryption techniques produce ciphers of the form; substitution ciphers, transposition ciphers, substitution-permutation ciphers, and machine ciphers. In substitution ciphers one alphabet is substituted for the other in the ciphertext. The transposition cipher shifts the position of the characters, and the substitution-permutation technique combines the substitution and permutation techniques. The machine cipher uses simple electromagnetic machines for the processing. These ciphers are broadly explained in the following sub sections

SUBSTITUTION CIPHERS

The first mathematical cipher was invented by the great roman emperor Julius Caesar, called Caesar cipher. The rule behind is for each plaintext, the corresponding ciphertext will be the one form its third position [Stallings, 05], [Menezes, 96], and [Sauerberg, 06].

The Playfair cipher [Stallings, 05], [Sauerberg, 06] invented by British Scientist Charles Wheatstone and Hill cipher [Hill, 29] developed by the mathematician Lester Hill are the best examples of monoalphabetic substitution ciphers. The monoalphabetic substitution ciphers expand the alphabet by introducing some extra characters so that, one plaintext letter is represented by more than one ciphertext character. These extra characters are known as randomizing elements and the process of expanding the alphabet is called homophonic coding / monoalphabetic substitution.

The Playfair cipher uses the Polybius square [5X5 matrix] with a keyword. In this the plaintext is split into digrams and each digram is encrypted as a separate entity. The Hill cipher encryption algorithm takes m successive plaintext letters and replaces them with m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1 ... z = 25). Ciphertext is computed by multiplying the key matrix with the plaintext matrix. And the decryption multiplies the inverse of key matrix with the ciphertext matrix. Here all processing is carried out with modular 26. ROT13 [Menezes, 96] is another substitution cipher which rotates each plaintext by 13 positions and rotating it again reveals the plaintext back.

The polyalphabetic substitution ciphers or the polyphones use a set of related monoalphabetic substitution rules. A key determines which particular rule is chosen for a given transformation. Vigenere Cipher [Stallings, 05] and [Sauerberg, 06], Beaufort Encryption [Sauerberg, 06], Vernam Cipher [Stallings, 05] and, one-time pad [Konheim, 07] are some of the examples of polyalphabetic substitution ciphers. These ciphers use different tabula recta for deriving the set of monoalphabetic substitution rules.

TRANSPOSITION CIPHERS

In a transposition cipher the plaintext remains the same, but the order of characters is shuffled around. Scytale cipher, rail-fence technique and the columnar transposition / permutation are few of the examples for transposition ciphers [Stallings, 05], [Menezes, 96], and [Sauerberg, 06].

The Scytale transposition cipher claimed to have been used by the Spartan military of ancient Greek. The soldiers wrapped their belt in a fixed dimensioned rod, wrote the message as of normal text, unwrapped and used it as if a normal belt. Thus they communicated in the war field securely.

In rail-fence technique [Sauerberg, 06], the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, the plaintext 'computer science' will become 'CMUESINEOPTRCEC' using a depth of two. The columnar transposition or the permutation cipher [Stallings, 05], [Sauerberg, 06] maps the message in a rectangle row by row, and then read off the message column by column, with the help of a key order. It can perform one or more rounds of encryption. For example, the plaintext 'have a nice day' with the key '3 1 4 2' will produce the ciphertext, 'ANDECYHAEVIA' in single round of encryption.

SUBSTITUTION-TRANSPOSITION CIPHERS

The substitution-transposition ciphers combine the substitution and transposition rules in a single cipher. These ciphers acted as the ancestors of the modern ciphers which combine the substitution and transposition rules with higher complexity. Alberti encryption [Henk, 05] and ADFGVX encryption system, invented by Fritz Nebel [Konheim, 07] are the best examples of classical substitution-transposition ciphers.

MACHINE CIPHERS

Crypto machines are electromagnetic machines for automatic encryption using a composition of mixed alphabet substitutions often performed by means of rotors. Rotor is a wheel, sitting on an axle and having on both sides a ring of contacts that are internally wired in such a way that they implement a permutation. The machine ciphers were broadly used in the World Wars I and II. Examples of machine ciphers are; Enigma (Germany), Hebern Electric Code Machine (USA), TypeX (Great Britain), SIGABA = M-134-C (USA), NEMA (Switzerland) and, Hagelin Machine [Konheim, 07], [Henk, 05].

MODERN TECHNIQUES

The modern techniques involve the use of computers and complex processing. The modern techniques can be classified into symmetric algorithms which include stream ciphers and block ciphers, and asymmetric algorithms. The symmetric encryption or the single-key encryption or secret

key encryption uses a single key/secret key for both encryption and decryption process. The algorithm used for decryption is just the reverse of the one used for encryption i.e., the process is symmetric. Stream cipher is one that encrypts a digital data stream one bit (or byte) at a time. Block cipher is one in which the plaintext is divided in blocks and one block is encrypted at one time producing a ciphertext of equal length. Table 2 gives the summary of the symmetric encryption algorithms.

The asymmetric encryption or the public-key encryption or the two-key encryption uses two keys; one for encryption and the other for decryption. Of the two keys one is kept secret and the other is published i.e., made public. Table 3 provides the summary of asymmetric algorithms.

AUTHENTICATION FUNCTIONS

The main goal of cryptography on its application through network is to achieve secrecy or confidentiality and authentication. Confidentiality is achieved through various encryption techniques applied over the data. To ensure authentication, mainly two techniques are used: the message authentication codes (MAC) and the hash functions [Stallings, 05], [Menezes, 96], [Konheim, 07], and [Henk, 05]. The MAC is the cryptographic checksum computed with the help of the message and a shared secret key, which is send along with the encrypted message and verified by the receiver. The Hash functions produces a fixed length message digest out of the original message, which is appended with the encrypted message and is also verified by the receiver to ensure integrity and authentication. Table 4 compares various hash algorithms.

BRANCHES OF CRYPTOGRAPHY

The following section details the widely known branches of cryptography, namely; Cryptographic Engineering, Multivariate Cryptography, Quantum Cryptography, Steganography, Visual Cryptography, Neural Cryptography and, DNA Cryptography, but a lot more are yet to bloom.

CRYPTOGRAPHIC ENGINEERING

Cryptographic Engineering [Koc, 09], [Cilardo, 06] is the theory and practice of engineering of cryptographic systems. This discipline uses cryptography to solve human problems; especially when trying to ensure data confidentiality, to authenticate people or devices, or to verify data integrity in risky environments. A cryptographic engineer designs, implements, tests, and validates cryptographic systems, also cryptanalyzes to check their strength against attacks, and to find the countermeasures. The essential aspects of cryptographic engineering are implementation efficiency and implementation security.

MULTIVARIATE CRYPTOGRAPHY

Multivariate Cryptography [Ding, 09] is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over finite fields. Solving systems of multivariate polynomial equation is proven to be NP-Hard [Menezes, 96] or NP-Complete [Menezes, 96]. Multivariate quadratics could be used to build signatures, and trials to build a secure encryption scheme are going on.

QUANTUM CRYPTOGRAPHY

The Quantum Cryptography [Bennett, 84], [Gisin, 02], [Bill, 03] emerged from the branch of Physics, Quantum Mechanics. It uses the quantum machines to do the cryptographic tasks, especially key generation. A good example is Quantum Key Distribution (QKD) which uses quantum machines to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can be used with any chosen encryption algorithm to encrypt and decrypt a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad.

STEGANOGRAPHY

Steganography [Stallings, 05], [Johnson, 1998] is the counter part of cryptography derived from the two Greek words; steganos meaning covered and graphos meaning I write or writing. Steganography is the art and science of masking/covering the presence of original message itself in a medium, and in cryptography the presence of message will be felt, but is in an unreadable form, protected from the unintended reader. Researchers used to say that the art of steganography existed even before the birth of cryptography.

The steganographic techniques can be broadly classified into linguistic steganography and technical steganography [Fabien, 99].

VISUAL CRYPTOGRAPHY

Visual Cryptography [Naor, 95] is a cryptographic technique which allows visual information such as pictures, text to be encrypted in such a way that decryption can be performed by the human visual system, without the aid of computers.

In 1994, Moni Naor and Adi Shamir demonstrated a visual secret sharing system, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image could appear.

NEURAL CRYPTOGRAPHY

Neuro-Cryptography [Neuro, 95], as introduced in 1995 or the Neural Cryptography [Kinzel, 02] gets the name by the use of artificial intelligence concept, neural networks in cryptosystems. The main feature of neural networks is the learning/ training process, by which they can selectively find the solution of a particular problem, making them a good choice for cryptanalysis. As they exhibit mutual synchronization property, they can be used for key management. Also, they are good choice for generation of hash values and can be used for key generation as they can produce pseudo-random numbers.

DNA CRYPTOGRAPHY

DNA contains the genetic instructions used in the development and functioning of all living organisms. It is composed of the most complex organic molecules and is essential for the identity of any organism. The main role of DNA molecules is the long-term storage of information, and hence DNA is called the hereditary material. DNA Cryptography [Gehani, 00], [Popovici, 10] has emerged with the research of Biomolecular Computation, which makes use of biotechnological methods such as DNA for doing computation. The DNA one-time-pads formed from the DNA strands are unbreakable and overcome the limitations of ordinary one-time-pad. Other DNA encryptions are; DNA based DES, RSA, XOR, etc. DNA cryptosystems are also used in steganography, watermarking, and also in cryptanalysis.

APPLICATIONS OF CRYPTOGRAPHY

Cryptic concepts play a vital role in day to day activities of human beings. The widely known applications are briefed in this section, which includes the digital signatures, electronic voting, financial cryptography etc.

COMMITMENT SCHEME

Commitment scheme [Brassard, 88], [Naor, 91] allows one to commit to a value while keeping it hidden, with the ability to reveal the committed value later. The commit and reveal are the two phases for interactions in a commitment scheme. The wider use of commitment scheme are; coin flipping [Blum, 83], zero-knowledge proofs [Goldreich, 91], [Goldreich, 96], and verifiable secret sharing [Feldman, 87], [Stadler, 96], which serves as the critical building block of secure multiparty computation.

SECURE MULTIPARTY COMPUTATIONS

Secure computation [Yao, 82] is the term introduced by Yao in early 1980s and it has evolved into a part of cryptography in these three decades. The problem behind secure computation can be stated as follows; “Consider a set of parties who do not trust each other, nor the channels by which they communicate. Still, the parties wish to correctly compute some common function of their local inputs, while keeping their local data as private as possible.” In short it can be stated as, “combining information while protecting it as much as possible.” Secure computation, if it involves only two parties, then it is called as Secure Two-Party Computation or simply Two-Party Computation. As well as, if more than two parties are involved, it is termed as Secure Multi-Party Computation or simply as Multi-Party Computation [Goldreich, 87]. The security requirements are; privacy – meaning that the parties involved in computation learn only the final output of the computation and nothing else, correctness or fairness – meaning that the output is correctly/ fairly distributed among the parties, and independence of inputs – meaning that the parties cannot make their inputs depending on the other parties’ inputs.

Construction of secure computation protocols follows two approaches (i) generic approach which relies on completeness theorems for secure computation, allows protocols for computing any function f starting from a circuit representation of the function, f (ii) second approach exploits the specific properties of a function to design special purpose secure computation protocols. Generic approach consists of garbled circuit construction followed by oblivious transfers. Exploiting specific

properties of functions approach uses verifiable secret sharing, homomorphic encryption etc. The fully homomorphic encryption proposed by Gentry [Gentry, 09] is an important enhancement in the exploiting specific properties of functions approach which has been developed into a fully functional library HELib by IBM in 2013 for secure computation. The problem of fully homomorphic encryption can be stated as follows; "One can arbitrarily compute on encrypted data, i.e., one can process encrypted data such as, querying, writing, or doing anything that can be efficiently expressed as a circuit, without the decryption key. And later on request, the process can be reversed so that the user can decrypt the data to retrieve the original data." Secure computation provides solutions to various real life problems such as, distributed voting, private bidding and auctions, sharing of signature etc.

DIGITAL SIGNATURE

Digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. The concept of digital signatures is closely related to the public-key cryptosystems. It started with the Diffie-Hellman key exchange algorithm [33] in 1976 and proceeded with digital signature standard [NIST, 09], authentication protocols by various persons including Denning, Needham, Woo and Lam [Clark, 97], and elliptic curve key exchange [Stallings, 05] etc.

FINANCIAL CRYPTOGRAPHY

Financial cryptography [Ian, 00] is the use of cryptography in applications in which financial loss could result from subversion of the message system. It appears to be a science, or perhaps an art, that finds its place at the intersection of previously unrelated disciplines such as, accountancy and auditing, programming, systems architecture, cryptography, economics, Internet, finance and banking, marketing and distribution etc. Financial cryptography can be explained with a seven layer model as follows.

L1 – Cryptography: consists of the mathematical techniques for secure communication

L2 – Software Engineering: consists of tools for communication over internet with reliability constant on nodes

L3 – Rights: consists of authentication details

L4 – Accounting: consists of framework which contains value within defined and manageable places

L5 – Governance: consists details on security of system from non-technical threats

L6 – Value: consists of the instruments that carry monetary or other value

L7 – Finance: consists applications for financial users, issuers of digital value, and trading and market operations

FC is closely related with the day to day applications such as ATMs, anonymous internet banking, electronic money, funds transfer etc.

Onion Routing

The concept of onion routing was developed by Michael and co. in 1998 [Reed]. It is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then

sent through several network nodes called onion routers. Each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where the same process is repeated. This prevents the intermediate nodes from knowing the origin, destination, and contents of the message.

Tor [Dingledine, 04], the second generation onion router was published in 13th August 2004. As of October 2009, there were about 1500 publicly accessible onion routers. Tor provides perfect forward secrecy and moves protocol cleaning outside of the onion routing layer, making it a general purpose TCP transport.

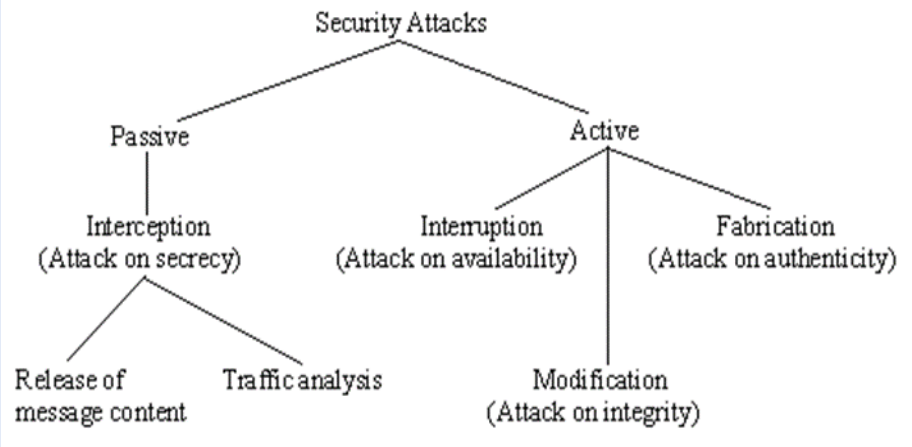
CLOUD COMPUTING SECURITY

One of the major obstacle for cloud computing is data confidentiality especially in public clouds. The common attacks on cloud computing are; denial of service, network sniffing etc. These attacks can be overcome by the use of virtual private clouds [Jamil, 11]. Multi-tenancy and virtualization [Mishra, 13] also enable security in cloud computing. Virtualized Firewall/VPN, Virtualized IDS/IPS, Hybrid Content Filtering, Hybrid Data Loss Prevention are few of the traditional security measures adapted to cloud computing to provide security and they are merely intermediate stages to a "anything – as – a – service" concept [Radut] of clouds.

CRYPTANALYSIS

Cryptanalysis [Stallings, 05], [Umich], [Kelsey, 98] or the code breaking is the study of methods for obtaining the meaning of encrypted information (ciphertext), without access to the secret information (key). In general, the cryptographic attacks can be broadly classified into two types; active attacks and passive attacks as shown in Figure 2. The attacks on encrypted message normally falls into one of the five categories depending on the amount of information known to the hacker; ciphertext only attack, known plaintext attack, chosen plaintext attack, chosen ciphertext attack, and chosen text attack [Stallings, 05]. The cryptanalysis on modern ciphers can be carried out with the help of linear cryptanalysis or differential cryptanalysis. The cryptanalysis on block ciphers is collectively described by Schneier [Schneier, 00].

Figure 2. Types of attacks.



CONCLUSION

In the information age, cryptography has become one of the major methods for protection in all applications. It is used not only over the Internet, but also in phones, televisions, and a variety of other household items. This paper attempts to brief the cryptographic techniques, both classical and modern to a reader in an easy and compact manner. Survey on various branches and applications of cryptography has been discussed to provide a fundamental understanding of the on-going research in this area.

ABBREVIATIONS

AES	: Advanced Encryption Standard
ATM	: Automated Teller Machine
CAST	: Carlisle Adams and Stafford Tavares
DES	: Data Encryption Standard
DNA	: DeoxyriboNucleic Acid
FC	: Financial Cryptography
FEAL	: Fast data Encipherment Algorithm
HAVAL	: Hashing Algorithm with Variable Length
ICE	: Information Concealment Engine
IDEA	: International Data Encryption Algorithm
IDS	: Intrusion Detection System
IPS	: Intrusion Prevention System
MD	: Merkle-Damgrad / Message Digest
NP	: Nondeterministic Polynomial time
RC	: Ron's Code or Rivest Cipher
RIPEMD	: RACE Integrity Primitives Evaluation Message Digest
RSA	: Rivest – Shamir – Adleman
SAFER	: Secure And Fast Encryption Routine
SHA	: Secure Hash Algorithm
TCP	: Transmission Control Protocol
TEA	: Tiny Encryption Algorithm
VPN	: Virtual Private Network

WAKE : Word Auto Key Encryption

XTEA : eXtended Tiny Encryption Algorithm

Table 2. Summary of symmetric encryption algorithms

Sl.No	Algorithm	Block Size	Key Size	Number of Rounds	Structure	Other properties and Applications
1	Feistel [Henk, 05]	64 bits	128 bits	16	Basic SPN structure	Most of the symmetric block ciphers follows its structure
2	AES [Daemen, 11]	128 bits	128, 192 or 256 bits	10, 12 or 14	SPN, but not Feistel network	Current symmetric encryption standard – Rijndael Cipher
3	BEAR [Anderson, 96-2]	Block size varies from 2^{13} to 2^{23} bits	160 bits for SHA1, and 128 bits for MD5	3	Unbalanced Feistel network	Uses the hash function and the stream cipher as round functions
4	Blowfish [Schneier, 94]	64 bits	Varies from 8 up to 448 bits	16	Feistel network	Key-dependent S-boxes and a highly complex key schedule, requires about 4 KB of memory
5	CAST-128 [Adams, 97]	64 bits	40 to 128 bits	12 or 16	Feistel network	Used in PGP
6	DES [Standard, 99]	64 bits	56 bits	16	Feistel network	FIPS PUB 46
7	FEAL [Shimizu, 88]	64 bits	64 bits	Initially 4, then 8, then variable (32)	Feistel network	Proposed as an alternative for DES
8	ICE [Kwan, 97]	64 bits	64 bits	16	Feistel network	Similar to DES with the addition of a key-dependent bit permutation in the round function
9	IDEA [Lai, 92]	64 bits	128 bits	8+1	SPN, but not Feistel	Developed as an alternative for DES, used in OpenPGP
10	MARS [Burwik, 98]	128 bits	128 to 448 bits	32	Type-3 Feistel network	One of the AES finalist

Sl.No	Algorithm	Block Size	Key Size	Number of Rounds	Structure	Other properties and Applications
11	Mercy [Crowley, 01]	4096 bits	128 bits	6	Balanced Feistel network	Used for fast disk sector encryption
12	RC2 [Rivest, 98]	64 bits	8 to 128 bits; default 64 bits	18	Source-heavy Feistel network	The 18 rounds are designed as, 16 mixing + 2 masking rounds
13	RC5 [Rivest L., 95]	32, 64 or 128 bits	0 to 2040 bits	1 – 255	Feistel like network	Key expansion uses one-way function with the binary expansions of ε and the *golden ratio*
14	RC6 [Rivest L., 98]	128 bits	128, 192 or 256 bits	20	Feistel network	AES finalist
15	SAFER [Massey, 94]	64 bits	64 bits	8	SPN	Uses the pseudo-Hadamard transform (PHT)
16	SEED [Lee, 05]	128 bits	128 bits	16	Nested Feistel network	Developed by the Korean Information Security Agency, and used broadly throughout South Korean industry
17	Serpent [Anderson, 98]	128 bits	128, 192 or 256 bits	32	SPN	AES finalist
18	TEA [Wheeler, 95]	64 bits	128 bits	Variable; recommended 64	Feistel network	Lightweight encryption algorithm
19	Triple DES [Kummert, 98]	64 bits	168, 112 or 56 bits	48	Feistel network	Increases the key size of DES by three times
20	Twofish [Schneier, 98]	128 bits	128, 192 or 256 bits	16	Feistel network	Uses pre-computed key-dependent S-boxes, and a relatively complex key schedule. Used in OpenPGP

Sl.No	Algorithm	Block Size	Key Size	Number of Rounds	Structure	Other properties and Applications
21	XTEA [Needham, 97]	64 bits	128 bits	Variable; recommended 64	Feistel network	Lightweight encryption algorithm designed to overcome the weakness of TEA
22	A5/1 [Henk, 05]	Stream 114 bits	64 bits	-	Uses three LFSRs	GSM mobiles
23	Grain [Hell, 07]	Bit oriented synchronous stream cipher	80 bits, IV – 64 bits	-	LFSR + NFSR + output function	For constrained environments such as Bluetooth and GSM
24	RC4 [Henk, 05]	Stream cipher	40 to 2048 bits	256	Uses state size of 2048 bits	Used in SSL, WEP
25	Salsa20/r; r = round [Salsa]	eStream cipher (software oriented)	128 / 256 bits	8, 12, 20 (12 is the best)	Uses ARX construction	Can generate output blocks upto 2^{70} bit in any order and in parallel, with comfortable margin of security
26	SNOW [Ekdahl, 00]	Stream 32-bit words	128 / 256 bits	-	LFSR + FSM	Group of word-based synchronous stream ciphers
27	SOSEMANUK [Sosemanuk]	eStream, synchronous stream cipher	128 to 256 bits with IV of 128 bits to produce 128 bit security	Can encrypt long data streams at 5.60 cycles/byte on Pentium machine	LFSR + FSM	Uses similar design principles to the stream cipher SNOW 2.0 and block cipher SERPENT, fixes drawbacks of SNOW2.0
28	Turing [Rose, 03]	Fast stream cipher	32 to 256 bits in multiples of 4 bytes	Maximum of 2^{160} – 160 bit blocks can be generate with a single key	LFSR + keyed mixing function	4K bytes of ROM is sufficient to yield very fast implementation
29	WAKE [Wheeler, 94]	Stream cipher	32 bit words	Has computation cost of 20 machine code instructions per word	Generates keystream blocks from previous ciphertext blocks	Uses an S-box with 256 entries of 32-bit words.

Table 3. Summary of asymmetric encryption algorithms

Sl.No	Algorithm	NP-Hard Problem	Details	Applications
1	Diffie-Hellman [Diffie, 76]	Discrete logarithm problem	Public-key cryptosystem invented with this algorithm in 1976	Used for key exchange
2	RSA [Rivest L., 78]	Factorization problem	PKCS#1 Current public-key encryption standard	Used for almost all public-key applications
3	Merkle–Hellman knapsack cryptosystem [Hellman, 80]	Subset sum problem	One-way kind of algorithm, public-key is used only for encryption and the private-key is used only for decryption	Used only for encryption
4	ElGamal encryption system [ElGamal, 85]	Based on Diffie-Hellman key exchange / discrete logarithm	Can be defined over a cyclic Group	ElGamal encryption is probabilistic; causes expansion of the rate of 2:1 from plaintext to ciphertext
5	Elliptic Curve Cryptography (ECC) [Simon, 12]	Discrete logarithm problem	ECC is based on the algebraic structure of elliptic curves over finite fields	Used in integer factorization algorithms applicable for cryptography, ECC key exchange, and for digital signature

Table 4. Summary of cryptographic hash functions

Sl.No	Algorithm	Message Digest Length in bits	Size of block processed in bits	Number of Steps	Maximum message size (bits)	Endianness
1	FORK-256 [Hong, 06]	256	512	4 parallel rounds of 8 steps	2^{64}	Big
2	GOST [Dolmatov, 10]	256	256	32	∞	Little
3	HAVAL [Zheng, 93]	128, 160, 192, 224, or 256	1024	3, 4, or 5 rounds of 32 steps	$2^{64} – 1$	Little
4	MD2 [Kaliski, 92]	128	128	18 rounds of 48 steps	∞	Irrelevant
5	MD4 [Rivest L., 91]	128	512	3 rounds of 16 steps	∞	Little
6	MD5 [Rivest L., 92]	128	512	4 rounds of 16 steps	∞	Little
7	MD6 [Rivest L., 08]	1 to 512	1024	Variable = 40 + integer part of message digest length/4	$2^{64} – 1$	Big

Sl.No	Algorithm	Message Digest Length in bits	Size of block processed in bits	Number of Steps	Maximum message size (bits)	Endianness
8	RIPEMD-160 [Dobbertin, 96]	160	512	5 pairs of 16 steps	∞	Little
9	SHA-1 [Jones, 01]	160	512	4 rounds of 20 steps	$2^{64} - 1$	Big
10	SHA-256 [NIST, 12]	256	512	64	$2^{64} - 1$	Big
11	SHA-384 [NIST, 12]	384	1024	80	$2^{128} - 1$	Big
12	SHA-512 [NIST, 12]	512	1024	80	$2^{128} - 1$	Big
13	SMASH-256 [Knudsen, 05]	256	512; sub-blocks use 256	12 H rounds, and 3 L rounds	$2^{128} - 1$	Irrelevant; suited for 32-bit architecture
14	SMASH-512 [Knudsen, 05]	512	1024; sub-blocks use 512	18 H rounds, and 5 L rounds	$2^{256} - 1$	Irrelevant; suited for 64-bit architecture
15	SWIFFTX [Arbitman, 08]	224, 256, 384, or 512	2048	3 parallel	$2^{64} - 1$	Irrelevant

Sl.No	Algorithm	Message Digest Length in bits	Size of block processed in bits	Number of Steps	Maximum message size (bits)	Endianness
16	Tiger [Anderson, 96-1]	192	512	24	$2^{64} - 1$	Little
17	Wirlpool [Barreto, 00]	512	512	10	$2^{256} - 1$	Irrelevant

REFERENCES

1. [Adams, 97] Adams, Carlisle: The CAST-128 encryption algorithm – RFC 2144, Entrust Technologies, May - 1997.
2. [Anderson, 96-1] Anderson, Ross, and Eli Biham: Tiger: A fast new hash function, In Fast Software Encryption, pp. 89-97, Springer Berlin Heidelberg, 1996.
3. [Anderson, 96-2] Anderson, Ross, and Eli Biham: Two practical and provably secure block ciphers: BEAR and LION, Fast Software Encryption. Springer Berlin Heidelberg, 1996.
4. [Anderson, 98] Anderson, Ross, Eli Biham, and Lars Knudsen: Serpent: A proposal for the advanced encryption standard, NIST AES Proposal, 1998.
5. [Arbitman, 08] Arbitman, Yuriy, Gil Dogon, Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen: SWIFFTX: A proposal for the SHA-3 standard, Submission to NIST, 2008.
6. [Barreto, 00] Barreto, P. S. L. M., and Vincent Rijmen: The Whirlpool hashing function, In First open NESSIE Workshop, Leuven, Belgium, vol. 13, p. 14. 2000.
7. [Bennett, 84] Bennett, Charles H., and Gilles Brassard: Quantum cryptography: Public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Vol. 175, No. 0, 1984.
8. [Bill, 03] Bill Grindlay: Quantum Cryptography – A study into the present technologies and future applications, 14th January 2003, Next Generation Security Software Ltd, www.ngssoftware.com
9. [Blum, 83] Blum Manuel: Coin Flipping by Telephone, Proceedings of CRYPTO 1981, pp. 11–15, 1981, reprinted in SIGACT News vol. 15, pp. 23–27, 1983
10. [Brassard, 88] Brassard, Gilles, David Chaum, and Claude Crépeau: Minimum disclosure proofs of knowledge, Journal of Computer and System Sciences 37.2: 156-189, 1988.
11. [Burwik, 98] Burwick, Carolynn, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas Jr et al., MARS-a candidate cipher for AES, NIST AES Proposal 268, 1998.
12. [Cilardo, 06] Cilardo, Alessandro, Luigi Coppolino, Nicola Mazzocca, and Luigi Romano: Elliptic curve cryptography engineering, Proceedings of the IEEE 94, no. 2, pp: 395-406, 2006.
13. [Clark, 97] Clark, John Andrew, and Jeremy Lawrence Jacob: A survey of authentication protocol literature: Version 1.0., 1997.
14. [Crowley, 01] Crowley, Paul: Mercy: A fast large block cipher for disk sector encryption, In Fast Software Encryption, pp. 49-63, Springer Berlin Heidelberg, 2001.
15. [Daemen, 11] Daemen Joan, Vincent Rijmen: A. E. S. Proposal – Rijndael, 2011, 1046-1049.
16. [Diffie, 76] Diffie W. and Martin Hellman: New Directions In Cryptography, IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976.
17. [Ding, 09] Ding, Jintai, and Bo-Yin Yang, Multivariate public key cryptography, In Post-Quantum Cryptography, pp. 193-241, Springer Berlin Heidelberg, 2009.
18. [Dingledine, 04] Dingledine, Roger, Nick Mathewson, and Paul Syverson: Tor - The second-generation onion router. NAVAL RESEARCH LAB WASHINGTON DC, 2004.
19. [Dobbertin, 96] Dobbertin, Hans, Antoon Bosselaers, and Bart Preneel: RIPEMD-160: A strengthened version of RIPEMD, In Fast Software Encryption, pp. 71-82. Springer Berlin Heidelberg, 1996
20. [Dolmatov, 10] Dolmatov, Vasily: GOST R 34.11-94: Hash Function Algorithm, 2010.
21. [Ekdahl, 00] Ekdahl, Patrik, and Thomas Johansson: SNOW-a new stream cipher, Proceedings of First Open NESSIE Workshop, KU-Leuven. 2000.
22. [ElGamal, 85] ElGamal, Taher: A public key cryptosystem and a signature scheme based on discrete logarithms, Information Theory, IEEE Transactions on 31.4, pp: 469-472, 1985.
23. [Fabien, 99] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: Information Hiding – A Survey, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7): 1062-1078, July 1999.
24. [Feldman, 87] Feldman, Paul: A practical scheme for non-interactive verifiable secret sharing, In Foundations of Computer Science, 1987., 28th Annual Symposium on, pp. 427-438. IEEE, 1987.
25. [Gehani, 00] Gehani Ashish, Thomas H. LaBean, and John H. Reif: DNA-based Cryptography, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 54, pp. 233-249, 2000.

26. [Gentry, 09] Gentry, Craig: A fully homomorphic encryption scheme, PhD diss., Stanford University, 2009.
27. [Gisin, 02] Gisin, Nicolas, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden: Quantum cryptography, Reviews of modern physics 74, no. 1, pp: 145-195, 2002.
28. [Goldreich, 87] Goldreich, S. Micali, and A. Wigderson: How to play ANY mental game, In Proceedings of the nineteenth annual ACM conference on Theory of computing, pages 218-229. ACM Press, 1987.
29. [Goldreich, 91] Goldreich, Oded, Silvio Micali, and Avi Wigderson: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems, Journal of the ACM (JACM) 38.3: 690-728, 1991.
30. [Goldreich, 96] Goldreich Oded and Hugo Krawczyk: On the Composition of Zero-Knowledge Proof Systems, SIAM Journal on Computing, 25: 1, pp. 169–192, 1996.
31. [Hell, 07] Hell, Martin, Thomas Johansson, and Willi Meier: Grain: a stream cipher for constrained environments, International Journal of Wireless and Mobile Computing 2.1: 86-93, 2007.
32. [Hellman, 80] Hellman, Martin E., and Ralph C. Merkle: Public key cryptographic apparatus and method, U.S. Patent No. 4,218,582. 19 Aug. 1980.
33. [Henk, 05] Henk C.A. van Tilborg: Encyclopedia of Cryptography and Security, ISBN-13: (eBook) 978-0387-23483-0, Springer, 2005
34. [Hill, 29] Hill S. Lester: Cryptography in an Algebraic Alphabet, The American Mathematical Monthly, Vol. 36, No. 6. (Jun. - Jul., 1929), pp. 306-312.
35. [Hong, 06] Hong, Deukjo, Donghoon Chang, Jaechul Sung, Sangjin Lee, Seokhie Hong, Jaesang Lee, Dukjae Moon, and Sungtaek Chee: A new dedicated 256-bit hash function: FORK-256, In Fast Software Encryption, pp. 195-209. Springer Berlin Heidelberg, 2006.
36. [Ian, 00] Ian Grigg: Financial Cryptography in 7 Layers, Proceedings of Financial Cryptography Fourth International Conference, Anguilla, British West Indies, 21st - 24th February 2000. A web copy is located at http://www.iang.org/papers
37. [Jamil, 11] Jamil, Danish, and Hassan Zaki: Cloud computing security, International Journal of Engineering Science and Technology 3, no. 4: 3478-3483, 2011.
38. [Johnson, 1998] Johnson, Neil F., and Sushil Jajodia: Exploring steganography: Seeing the unseen, IEEE computer 31.2: 26-34, 1998.
39. [Jones, 01] Jones, Paul E.: US secure hash algorithm 1 (SHA1), 2001.
40. [Kaliski, 92] Kaliski, B.: RFC 1319-The MD2 Message-Digest Algorithm, April 1992, RSA Laboratories.
41. [Kelsey, 98] Kelsey, John, Bruce Schneier, David Wagner, and Chris Hall: Side channel cryptanalysis of product ciphers, In Computer Security—ESORICS 98, pp. 97-110. Springer Berlin Heidelberg, 1998.
42. [Kinzel, 02] Kinzel, Wolfgang, and Ido Kanter: Neural cryptography, In Neural Information Processing, 2002. ICONIP'02. Proceedings of the 9th International Conference on, vol. 3, pp. 1351-1354. IEEE, 2002.
43. [Knudsen, 05] Knudsen, Lars R.: SMASH–a cryptographic hash function, In Fast Software Encryption, pp. 228-242, Springer Berlin Heidelberg, 2005.
44. [Koc, 09] Koç, Cetin Kaya: About Cryptographic Engineering, Springer US, 2009.
45. [Konheim, 07] Konheim G. Alan: Computer Security and Cryptography, John Wiley & Sons, 2007
46. [Kummert, 98] Kummert, Holger: The PPP Triple-DES Encryption Protocol (3DESE), RFC 2420, 1998.
47. [Kwan, 97] Kwan, Matthew: The design of the ICE encryption algorithm, Fast Software Encryption, Springer Berlin Heidelberg, 1997.
48. [Lai, 92] Lai, Xuejia: On the design and security of block ciphers, PhD diss., Diss. Techn. Wiss ETH Zürich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. Bühlmann, 1992.
49. [Lee, 05] Lee, Jaeil, Jongwook Park, Sungjae Lee, and Jeeyeon Kim: The SEED encryption algorithm, SEED-RFC 4009, 2005.
50. [Massey, 94] Massey, James L.: SAFER K-64: A byte-oriented block-ciphering algorithm, Fast Software Encryption, Springer Berlin Heidelberg, 1994.
51. [Menezes, 96] Menezes J. Alfred, Paul C. van Oorschot, Scott A. Vanstone: Handbook of Applied Cryptography, Egdlectronic version, 1996
52. [Mishra, 13] Mishra, Ankur, Ruchita Mathur, Shishir Jain, and Jitendra Singh Rathore: Cloud Computing Security, International Journal on Recent and Innovation trends in Computing and Communication 1, no. 1, pp: 36-39, 2013.

53. [Naor, 91] Naor, Moni: Bit commitment using pseudorandomness, Journal of cryptology 4.2: 151-158, 1991.
54. [Naor, 95] Naor, Moni, and Adi Shamir: Visual cryptography, In Advances in Cryptology—EUROCRYPT'94, pp. 1-12. Springer Berlin Heidelberg, 1995.
55. [Needham, 97] Needham, Roger M., and David J. Wheeler: Tea extensions, 1997.
56. [Neuro, 95] Neuro-Cryptography 1995 - The first definition of the Neuro-Cryptography (AI Neural-Cryptography) applied to DES cryptanalysis by Sebastien Dourlens, France.
57. [NIST, 09] FIPS, PUB. 186-3. Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), 2009.
58. [NIST, 12] PUB, NIST FIPS, 180-4 Secure Hash Standard, March 2012.
59. [Popovici, 10] Popovici Calina, Aspects of DNA Cryptography, Annals of the University of Craiova, Mathematics and Computer Sciene Series, Volume 37(3), pp.147-151, 2010.
60. [Radut] RADUT, Carmen, Ionela POPA, and Diana CODREANU: CLOUD COMPUTING SECURITY, REVISTA ECONOMICĂ: 171.
61. [Reed] Reed Michael G., Paul F. Syverson, David M. Goldschlag: Onion routing network for securely moving data through communication networks, United States Patent – 6266704
62. [Rivest L., 08] Rivest, Ronald L., Benjamin Agre, Daniel V. Bailey, Christopher Crutchfield, Yevgeniy Dodis, Kermin Elliott Fleming, Asif Khan et al.: The MD6 hash function–a proposal to NIST for SHA-3, Submission to NIST 2 (2008): 3.
63. [Rivest L., 78] Rivest, Ronald L., Adi Shamir, and Len Adleman: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21, no. 2, pp: 120-126, 1978.
64. [Rivest L., 91] R.L. Rivest, The MD4 Message Digest Algorithm, Advances in Cryptology, Proc. Crypto'90, LNCS 537, S. Vanstone, Ed., Springer-Verlag, 1991, pp. 303-311.
65. [Rivest L., 92] Rivest, Ronald L.: RFC 1321: The MD5 message-digest algorithm, pp: 20-21, 1992.
66. [Rivest L., 95] Rivest, Ronald L.: The RC5 encryption algorithm, In Fast Software Encryption, pp. 86-96, Springer Berlin Heidelberg, 1995.
67. [Rivest L., 98] Rivest, Ronald L., Matt JB Robshaw, Ray Sidney, and Yiqun L. Yin: The RC6 block cipher, In in First Advanced Encryption Standard (AES) Conference, 1998.
68. [Rivest, 98] Rivest, Ron: A Description of the RC2 (r) Encryption Algorithm, RFC 2268, 1998.
69. [Rose, 03] Rose, Gregory G., and Philip Hawkes: Turing: A fast stream cipher, In Fast Software Encryption, pp. 290-306. Springer Berlin Heidelberg, 2003.
70. [Salsa] Salsa20/12, http://www.ecrypt.eu.org/stream/e2-salsa20.html
71. [Sauerberg, 06] Sauerberg, Jim: Cryptology: An Historical Introduction DRAFT, 2006.
72. [Schneier, 00] Schneier B.: Self-Study Course in Block Cipher Cryptanalysis, Cryptologia, v.24, n.1, pp. 18-34, Jan 2000.
73. [Schneier, 94] Schneier, Bruce: Description of a new variable-length key, 64-bit block cipher (Blowfish), Fast Software Encryption. Springer Berlin Heidelberg, 1994.
74. [Schneier, 98] Schneier, Bruce, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson: Twofish: A 128-bit block cipher, NIST AES Proposal 15, 1998.
75. [Shimizu, 88] Shimizu, Akihiro, and Shoji Miyaguchi: Fast data encipherment algorithm FEAL, Advances in Cryptology—EUROCRYPT'87, Springer Berlin Heidelberg, 1988.
76. [Simon, 12] Simon Blake-Wilson: Standards for Efficient Cryptography, Sec1: Elliptic Curve Cryptography, S. E. C. G. Std. "SEC1, 2000." 2012.
77. [Sosemanuk] SOSEMANUK, http://www.ecrypt.eu.org/stream/e2-sosemanuk.html
78. [Stadler, 96] Stadler, Markus: Publicly verifiable secret sharing, In Advances in Cryptology—EUROCRYPT'96, pp. 190-199. Springer Berlin Heidelberg, 1996.
79. [Stallings, 05] Stallings William: Cryptography and Network Security Principles and Practice, Fourth Edition, Prentice Hall, 2005, eText ISBN-13: 978-0-13-187319-3
80. [Standard, 99] Standard, N. F.: Data Encryption Standard, Federal Information Processing Standards Publication, 1999.
81. [Umich] Cryptanalysis, Basic. FM 34-40-2. FIELD MANUAL, DEPARTMENT OF THE ARMY http://www.umich.edu/~ umich/fm-34-40-2.
82. [Wheeler, 94] Wheeler, David J.: A bulk data encryption algorithm, In Fast Software Encryption, pp. 127-134, Springer Berlin Heidelberg, 1994.

83. [Wheeler, 95] Wheeler, David J., and Roger M. Needham: TEA, a tiny encryption algorithm, In Fast Software Encryption, pp. 363-366, Springer Berlin Heidelberg, 1995.
84. [Yao, 82] Yao Andrew Chi-Chih Protocols for Secure Computations (Extended Abstract) FOCS, pp: 160-164, 1982.
85. [Zheng, 93] Zheng, Yuliang, Josef Pieprzyk, and Jennifer Seberry: HAVAL—A one-way hashing algorithm with variable length of output, In Advances in Cryptology—AUSCRYPT'92, pp. 81-104. Springer Berlin Heidelberg, 1993.

About the Author:

Ms. Anasuya Threse Innocent [CSI - I0115810] has completed her M.E. in Computer Science and Engineering in 2002 and has around 8 years of working experience as Assistant Professor in reputed institutions. She has joined as a full time Research Scholar with Amrita University – Bangalore in 2012, and is doing her research in Secure Computation. She is a life member of CSI since 2004.

BLUE EYE TECHNOLOGY

Compiled by:

Hemalatha. L, V.Subedha and S.Hemalatha

PC TO IDENTIFY EMOTIONS

Can your PC identify your emotions (sad/happy/excited/surprised).Dryer (1999) has shown that people view their computers as having a personality ,thus its important for a computer to work well with its user, Here blue eye technology comes into force. Blue eye technology is a concept which aims to sense and identify human emotion level .

Artificial intelligence is a concept to create intelligence to machines. It does the work which is assigned to it, but intelligence alone cannot make the machine perfect, they can never understand the emotions of a human body, this blue eye technology aims in understanding the emotions to reduce and avoid human limitations such as oversight, tiredness in a long drive ,mental illness and for the ability to gather information about you and interact with you for eg: you can see your computer playing the favorite movie of yours, songs to cheer u up when your sad, interact with you, feel your presence, emotional intelligence concept to reduce accidents by identifying the emotional state of a driver based on deducting him facial emotions .it senses your emotion level by the elements like speech, eyes, fingers to sense your emotional level

CONCEPTS IN BLUE EYE TECHNOLOGY

Blue eye technology uses image processing techniques, it extracts the eye portion from the current image with the previous images stored in database and deducts the human emotions. it is achieved byunderstanding your emotions by using special techniques such as facial/Speech recognition, etc. To identify actions of a user and extract key information sensing technology is used, with this information it analyze and determine the users physical emotional state by performing the expected action or information eg: blue eye enabled television could become active when the user make eye contact at which point the user could then tell the tv to turn on .

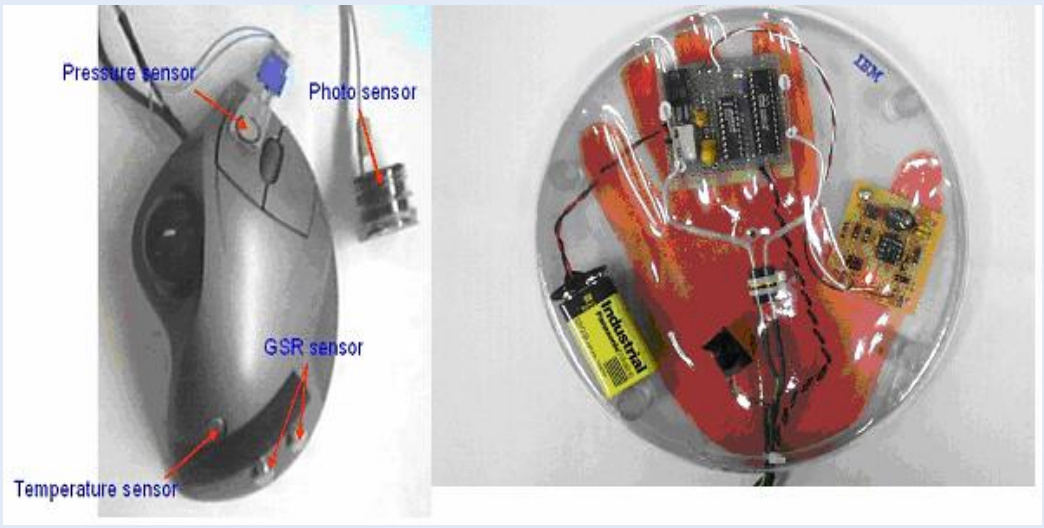
Actual working is achieved by a concept MAGIC It takes input from both the manual input and eye tracking system running either on same or different system connected via serial port .

Input from manual i/p device+ information from eye tracker = MAGIC pointing procedure

In MAGIC pointing it selects a manual control task but its aided by gaze tracking . the main idea is to gaze to dynamically wrap then home position of a pointing cursor to be at the vicinity of the target which can presumably what the user looking at , thereby effectively reducing the cursor movement

amplitude .once cursor is refined the user need to only make a small movement to and click on the target with the regular manual input device.

For Hand

- Emotions Mouse
- Sentic Mouse
- 

The information we get from emotional mouse are

1. Behavior
   - **Mouse movements**
   - **Button click frequency**
   - **Finger pressure** when a user presses his/her button
2. Physiological information
   - **Heart rate** (Electrocardiogram(ECG/EKG),
   - Photoplethysmogram(PPG))
   - **Skin temperature** (Thermester)
   - **Skin electricity** (Galvanic skin response)

ADVANTAGES:

It is a more natural mental model for the user to interact and communicate ,A PC with effective communication, quality, responsiveness with customers, Prevention from dangerous incidents, Physiological condition monitoring, Operators position detection, The course of operator's work is reconstructed

DISADVANTAGES:

Doesn't predict nor interfere with operator's thoughts, Cannot force directly the operator to work

FUTURE WORK:

In the near future ,ordinary household devices- devices(television , refrigerators, ovens) will be able to do our jobs when we look at them and speak to them. Blue eye technology's future applications will boom the market.

About the Authors:

Hemalatha is final year B.E Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. V. Subedha is Professor and Head of Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. S. Hemalatha is Professor, Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

CLOUD COMPUTING

Compiled by:

Sanjana Elsa Jose and Shahnaz K Nassar

ABSTRACT

This describes about the development of technology and using cloud computing we can share resources over the internet. In this we come across different uses of cloud computing, different components of cloud computing, different applications of cloud computing and the future of cloud computing and about Mobile Cloud Computing (MCC).

INTRODUCTION

Cloud computing is a type of procedure that relies on sharing computing resources. In simple words, Sharing computing on internet or sharing of computing services over the internet**.** Cloud computing is similar to grid computing. Cloud computing is used to perform complicated calculations within seconds. It is commonly used for military and research facilities. With the help of cloud computing we can save large amount of time. To do this, cloud computing uses large group of network of servers normally running on low-cost consumer PC technology with particular connections to spread data-processing tasks across them. This sharing IT infrastructure contains large groups of systems that are connected together. Often, different techniques like virtualization are used to increase the strength of cloud computing**.**

CLOUD COMPONENTS

1. Client computer

2. Distributed Servers

3. Datacenters

CLIENT COMPUTER

Clients are the tools that the end users communicate with cloud.

Three types of clients:

1. Mobile

2. Thick

3. Thin

DATACENTER

It is combination of servers where request is given and is retrieved through internet.

DISTRIBUTED SERVER

Often servers are placed in different areas but they behave like they are placed nearer to each other.

WHY CLOUD SERVICE IS POPULAR?

1. Minimize the difficulty of networks.
2. Doesn't have the need of buying software licenses.
3. Customization.
4. Cloud providers that have concentrated in a special area can bring latest services that a single company might not be able to provide or increase.
5. Expandable, dependable and competency.
6. Information's in cloud are safe.

APPLICATION

1 .Social networking sites.

2. E-mail sites.

3. Search Engines.

4. Many more services over the internet

THE FUTURE

Cloud computing is still a research topic. The significant cloud technology developers continue to invest billions a year in cloud. In 2011 Microsoft committed 90% of its budget to its cloud. This expansion also includes Finance and Accounting Software as a service (SaaS). Additionally, more industries are turning to cloud technology as an efficient way to improve different quality services due to its capabilities to reduce overhead costs, downtime, and automate infrastructure deployment.

MOBILE COMPUTING

Mobile Cloud Computing (MCC) is the mixture of cloud computing, mobile computing and wireless networks to bring productive computational assets to mobile users, network operators, as well as cloud computing providers. The greatest goal of MCC is to enable execution of rich mobile applications on a large number of mobile devices, with a much understandable user experience. MCC provides business opportunities for mobile network operators as well as cloud providers. More inclusively, MCC can be defined as "a rich mobile computing technology that borrows unified elastic resources of various clouds and network technologies toward not restricted functionality, storage, and mobility to serve a crowd of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of different environments and platforms based on the pay as you use assumption."

CONCLUSION

To summarize, the cloud provides many options for the everyday user .It opens up a vast area of computing to a broader range of uses and increases the ease of use by giving access through any internet facilities. However, with this increased ease also come drawbacks. You have limited control over who has access to your data and little to no knowledge of where it is stored. You also must be cautious of the security risks of having information stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection. If you are considering using the cloud, be certain that you identify what information you will be putting out in the cloud, who will have access to that information, and what you will need to make sure it is protected. Additionally, know your options in terms of what type of cloud will be best for your needs, what type of provider will be most useful to you, and what the reputation and responsibilities of the providers you are considering are before you sign up.

REFERENCES

1. www.webopedia.com
2. www.wikinvest.com
3. www.rackspace.com
4. Books- Architecting the Cloud
5. www.cloudendure.com

ACKNOWLEDGEMENT

We **Shahnaz K Nassar** and **Sanjana Elsa Jose** thank **G**od Almighty, our parents, our Institution - **A**mrita **S**chool of **A**rts and **S**ciences and our subject coordinators for giving us this opportunity for presenting our presentation. Last but not the least we also thank **C**omputer **S**ociety of **I**ndia (**CSI**) for organizing such an event which will help us to study more about the upcoming technologies and inventions.

About the Authors:

Sanjana Elsa Jose

sanjuelsataylor@gmail.com

CSI: 01333138

SHAHNAZ K NASSAR

ambily.shahnaz@gmail.com

CSI: 01333139

CYBER FORENSICS

Compiled by:

Priya. P , T. Kalaichelvi, S.Hemalatha

INTRODUCTION

Forensics computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is acceptable legally. Cyber forensics having some characteristics identifying, preserving, analyzing and presenting

NEEDS OF CYBER FORENSICS

1. To produce the evidence in the court that can lead to the punishment of the actual.
2. To focus on the response to hi-tech offenses, started to intertwine
3. To ensure the integrity of the system.

GOALS OF CYBER FORENSICS

The main goals of cyber forensics experts is not only to find out the evidence and presentation of the evidence but also to find the criminal in a manner that leads to legal action of the criminal.

APPLICATION OF CYBER FORENSICS

Cyber forensics applications are financial criminal prosecution, detection of fraud, civil litigation and corporate security policy then acceptable use violations.

ADVANTAGE OF CYBER FORENSICS

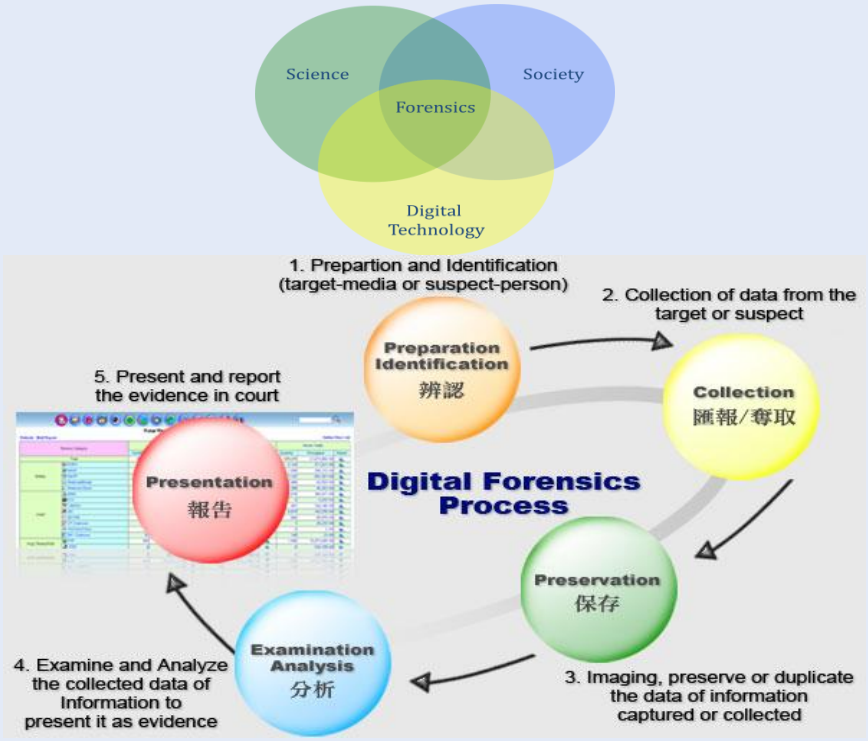
Computer forensics main **advantage is its quickly and efficiently ability to search and analyze a mountain of data.** They can search keywords in a hard drive in different languages through the internet which is beneficial since cybercrimes can easily cross borders.

DISADVANTAGE OF CYBER FORENSICS

The main disadvantage is the retrieving data cost. Analysis and reporting of data can take as long as 15 hours but it will also depend on the nature of the case. Computer forensic experts hire

per hour. Another one is that, analyst may inadvertently disclose privilege documents, when retrieving data.

LATEST TRENDS



DIGITAL FORENSICS

Digital forensics is problematical, any crime where computer is a tool, target or both offences against computer system or data. It is unauthorized access modification impairment of a computer or digital system. For example spam, phishing, man in the middle, denial of service.

Cyber forensics currently faces challenges as it struggles to keep pace with cyber-criminals. We can accelerate our cyber-crime prevention efforts and enhance the support.

About the Authors:

Priya. P, final year B.E Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. T. Kalaichelvi, Professor Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. S. Hemalatha, Professor ,Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

FLS: SIGNAL GENERATION FOR CONGESTION DETECTION AND PREVENTION IN ADAPTIVE NETWORKS

Compiled by:

K.Rangaswamy and Pandurangan Ravi

ABSTRACT

Identifying the occurrence of congestion in a network is a major task. In this paper describes detection and prevention of congestion, in general networks consists of routers and transmission line. Now a day's every data transmission will be done through network only, so that network usage rapidly growth ultimately congestion problem is arised. Due congestion network performance is decreases, Still there no proper solution. This paper proposed NEW techniques for detection and prevention of the congestion. The router will be carry the packets from one to another, before transmit data once send one FUTURE LEARNING SIGNAL (FLS) to its neighbors. If the Neighbor suffers with congestion then the sender router stops the data transmission for while or choose next alternative path to reach same destination.

INTRODUCTION

In dynamic Networks don't have a fixed infrastructure; it is a collection of notes and transmission lines. In a network each node acts as a router, which helps forwarding the packets from source to destination. In OSI reference model congestion control is the responsibility of the transport layer. However recent research has found that the users‟ access speed has increase and thus affects the efficiency of the network. New techniques are required to improve the efficiency of network traffic. The current assumption the networking research effects on individual network flow quality of service. Including loss of the packet, variation of delay time and wastage of the bandwidth. One way to reduce the load on the router is to increase the Maximum Transmission Unit (MTU) of the network. The data packet length exceeds the MTU then applies fragmentation method and divided into equal length of packets and inject to the network. The major problem is to find the appropriate route path to respective destinations and a network or geographical areas with more overhead for add on responsibility. If any drop of data, warning bit used to create the traces for data and will complete the duplicity of data. This mechanism will avoid big overhead which is introduced due to complete duplicate copy of data with each vehicular node agent so to decrease the congestion. The main objective is control the congestion by monitoring the network, if any problem in the network pass the information and solve the problem. This paper we introduce FLS Signal to detect the congestion and control the congestion. We are considering best-effort connectionless packet-switched networks where link capacity is typically fixed. Given that link bandwidth (and hence overall bit rate) is fixed, network operations which deal with bit rates may be useful. For example, if routers can feed back rate information to sources of traffic flows, then the routers can participate in the fair allocation of link capacity. Transport protocols which are rate-based can admit packets into the network uniformly spaced: this helps to prevent short-term congestion. Combined, these

techniques can be used as a form of congestion control, by allocating rates to traffic flows which keep network operation at the knee-point of peak power.

RELATED WORK

1. Congestion Detection: Set the minimum and maximum threshold value of queue length.
2. The minimum is 0.35 of buffer size.
3. The maximum is 2*0.35 minimum of buffer size.

Case 1: If the queue status is < minimum threshold.

The incoming traffic is low and queue is in safe zone.

Case2: The queue status > minimum threshold and Inst_queue < maximum threshold.

The incoming traffic is normal and queue is in congested zone.

Case3: Inst_queue>maximum threshold.

The incoming traffic is heavy and queue is in congested zone.

ROUTE DISCOVERY

Before the transmission of packet from source to destination, suppose intermediate node suffer from the congestion it generate warning signal to its predecessor and successors nodes. These nodes are attempt to identify the alternative path destined for destination. In the dynamic network the routers make dynamic path towards the destination.

DYNAMIC ROUTING ALGORITHM

In Dynamic environment router make independent path from source to destination. In Adaptive method every data packet having full length of address. Best dynamic algorithm is:

LINK STATE ALGORITHM

The main principles of link state algorithm Each router keeps a topology database of whole network link state updates flooded, or multicast to all network routers compute their routing tables based on topology often uses Dijkstra's shortest path algorithm. Mainly it consists of several operations in link state algorithm:

Step1: Finding of routers which are physically connected to the routers and also its IP address. When router starts working it will send the “HELLO” packet over the network. All routers within the network will receive the message its replays the ip address of that particular router.

Step2: Delay time for the neighboring routers in the network will be measured. Routers will send the Echo packets over the network, every router that receives these packets replies with an Echo reply Packet. By dividing the Round Trip Time by 2, routers can count the delay time. The Round Trip Time is a measure of the current delay on a network, found by timing a packet bounced off some

remote host. This time includes the time in which the packets reach the destination and the time in which the receiver processes it and replies.

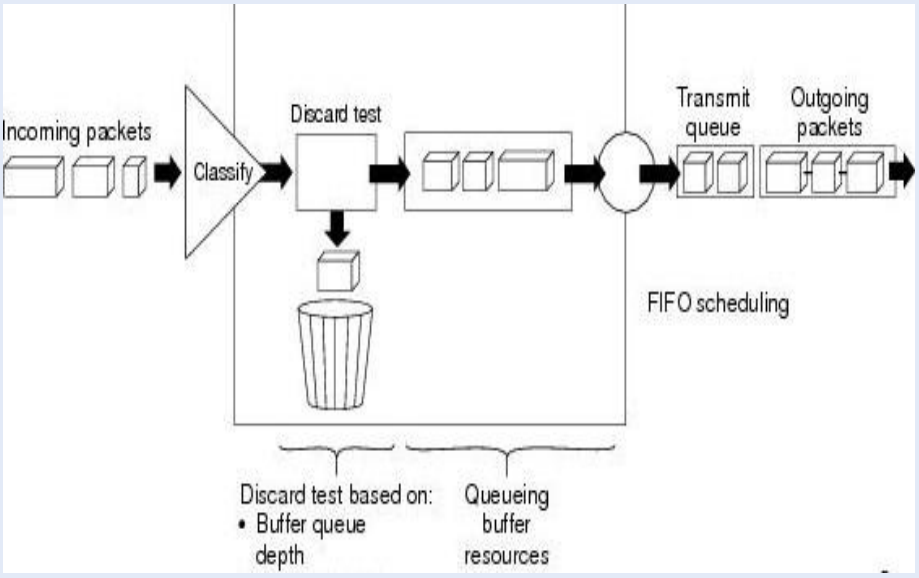
Step3: Router will broadcast all its information over the network for other routers and receives .Thus all routers share their knowledge and broadcast their information to each other and each router is acquainted with the structure and the status of the network.

Step4: The router will evaluate the best route between two nodes of network. Thus the best route for the packets to every node is chooses. For this evaluation the shortest path algorithm of Dijkstra is performed.

SIGNAL BASED CONGESTION DETECTION AND CONTROL

Network is a telecommunications network that allows computers to exchange data. Networked computing devices pass data to each other along data connections. Data is transferred in the form of packets. Before send the packet calculate distance between the neighbors based on this distance measure the FLS signal life time. Signal generation process is like CSMA/CD. Here also send the Carrier sense signal before send actual data, if channel is free transmission is done otherwise wait some random amount time. but in network layer if router congested instead of waiting check other alternative router to send packets. A packet consists of two kinds of data: control information and user data. The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between.

SAMPLE PACKET TRANSMISSION PROCESS:



CONGESTION ESTIMATION

Congestion in a network signifies that a node at any interval became congested and started to lose packets. Several metrics are available to monitor the congestion status at node level. For instance, it could be based on the average queue length and the percentage of packets discarded for lack of buffer space. Every second, a node checks the occupancy of its link layer queue using the dynamic congestion estimation technique so as to detect congestion well in advance. The dynamic congestion

(DC) estimation technique is a queue management algorithm that makes use of a direct measurement of the congestion status. In this situation, our algorithm introduces the Queue_utilization parameter, which will help to change the Maxth values dynamically until the alternative path discovery becomes true. We used expression (5) to get Queue_utilization value (Minth= 35% Queue_size; Maxth= 70% Queue_size; and Queue_utilization = 87.5% Queue_size), which consists of three ranges. It varies from 85% to 90% queue size with 2.5% difference. Finally, if the average queue length is greater than Maxth, then node‟s congestion status becomes Zone-III (congested zone). The algorithm for dynamic congestion estimation is shown in Algorithm I.

FLS GENERATION AND PERFORMANCE

Before transmission of any data need to check either the neighboring routers are healthy or not. To check the status of it in this paper introduced one FLS signal, The signal generate two kinds of responses.

Case I:

Initially send the FLS signal of its neighbor, Every signal have some lifetime, calculation of the life time is depends on distance if its neighbor. If the signal carries congestion free signal back to the sended router then free to transmit the packet.

Case II:

If the signal has negative response, router again follows two conditions:

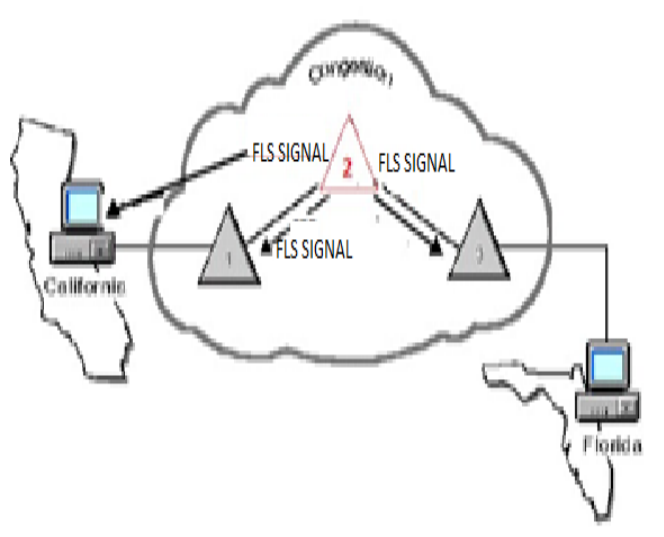
II.I : repeat case I, choose alternative congestion free path

If the path is found transmit immediately.

II-II: router wait for some random amount of time.

FLS signal generate when the router congested and the signal forward to their neighbours and directly transmit to sender. The sender check the status of FLS signal

show the information about present list of the packets in the router buffer, if buffer is become overflow then sender give rating for the buffered packets, that message forward to the congested router with help of urgent pointer.



Algorithm : Send FLS its neighbor node

Input Signal S = (cong_status, src_addr, dst_addr) to all the Valid entries.

The signal life time is Calculated by distance of distance of its neighbor.

/* Src: source node; Dst: destination Node; Cong_status – neighbour

Congestion status*/ Begin

Construct new node set from current node to destination Call route discovery process

/* find a new route from current node to destination */ Update new node set and add to all two hop neighbours Node‟s routing table

If SetRoute=True

Transmission is done

Else

Wait…

End

CONCLUSION

We have proposed a FLS signal to control the congestion. Network characteristics like congestion and route failure need to be detected and remedied with a reliable mechanism. To solve the congestion problem, we have proposed a dynamic congestion estimation technique(FLS) that could analyze the status of its neighbors. By having early detection of the buffer, we can initiate the process of the feedback to control the congestion. This scheme is better as compare to the waiting for congestion to happen and then to take corrective action.. This will aid the conveyance of the FLS signal to reach up to the neighbouring nodes.

REFERENCES

1. Braden, B., Clark, D., Crow croft, J., Davie, B., Eering, S., Estrin, D., Floyd, S., Jacobson, V.,Minshall, G., Partridge, C., Peterson, L., Ramakrishna, K., Shenker, S., Wroclaw ski, J., Zhang, L.,1998. Recommendations on queue management and congestion avoidance in the internet. RFC 2309, IETF.
2. Senthilkumaran, T., Sankaranarayanan, V., 2010. Early detection congestion and control routing in MANET, In: Proceedings of the Seventh IEEE and IFIP International Conference on Wireless and Optical Communications Networks (WOCN 2010), Srilanka, pp. 1–5.
3. Senthilkumaran, T., Sankaranarayanan, V., 2011b. Early congestion detection and optimal control routing in MANET. European Journal of Scientific Research 63 (1), 15–31.
4. Research on Traffic Monitoring Network and its Traffic Flow Forecast and Congestion Control Model Based on Wireless Sensor Networks. Xiao Laisheng, Peng Xiaohong College of Information Technology Guangdong Ocean University Zhanjiang, P.R. China Wang Zhengxia College of Law Guangdong Ocean University Zhanjiang, P.R. China 2009 International Conference.
5. Chieh-Yih Wan, Shane B. Eisenman and Andrew T. Cambell, “CODA: Congestion Detection and Avoidance in Sensor”, in Proc. of ACM SenSys‟03.
6. Computer network, S.Tanenbaum, fourth edition, Pearson education.
7. D.Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture, Prentice Hall, 2006.

Mr. K.Rangaswamy is currently an Assistant Professor of Computer Science and Engineering at Chaitanya Bharathi Institute of Technology Proddatur, Andrapradesh.His most focus on networks. Currently pursuing Ph.D in the area of networking at Bharath University .He received M.Tech degree in Computer Science at Bharath University, Chennai in 2011, his B.Tech degree in Computer Science and Engineering from JNTUA Anatapuramu in 2009.

Prof. Pandurangan Ravi has an experience of about 20 years in Teaching and as well as various Administrative positions at different organizations. After obtaining his undergraduate, Post Graduate and Doctoral Degree, he is now concentrating in the area of Computer Networks. He has published 8 Research Papers in International Journals and 4 in National and International Conferences. He is recipient of international Kohinoor Award for Educational Excellence” for the year 2010. He received the award “Mother Theresa Educational Excellence Award-2012” and also he received “International Researcher” for the year 2013 from IAMURE, Indonesia. He is life member of "Indian Society for Technical Education‟ and he is on editorial board for four International Journals.

GESTURE BASED AUDIO/VIDEO PLAYER

Compiled by:

Indrajeet Vadgama, Yash Khot, Yash Thaker, Pranali Jouras and Yogita Mane

ABSTRACT

In this project we have wish to develop a Windows-based application for live motion gesture recognition using web-cam as input built using Java, and using this input to control a video/audio player. This project is a combination of live motion detection and gesture identification. This application uses the webcam to detect gestures made by the user and perform basic operations## accordingly.

INTRODUCTION

In this project we propose a system to control VLC media player without physical interaction with the computer.

This is achieved by Java code using OpenCV libraries and using the inbuilt web-camera in laptops or external web-cameras for desktops.

OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in the commercial products. It has C++, C, Python, Java and MATLAB interfaces and supports Windows, Linux, Android and Mac OS.

Image is captured and verified with the application in which image pre-processing and other techniques are used for detection of gesture.

INPUTS

Image is captured and provided as the input to the application via a camera of minimum 1mp quality for good results.

PROCESSING

Processing will take place in the system after providing the input as image. Here the input gesture will be recognized on the basis of finger count.

OUTPUTS

The desired action will be performed.

ERROR HANDLING

Errors may arise due to invalid gestures or quick movement of hand resulting in the system not recognizing the gesture. Invalid gestures will result in no action being performed similarly quick movement of hand will be ignored to avoid accidental gestures.

EXISTING SYSTEMS

Existing systems on this domain do exist they are as follows,

- ArcSoft
- GestureTek

The existing systems on this domain use sensors or c# for implementation. Most laptops or personal computers do not come acquitted with sensors for this purpose, albeit web-cameras are very common.

LITERATURE SURVEY

N.Krishna Chaitanya and R.Janardhan[1] - defines Controlling of windows media player using hand recognition system.

***Disadvantage**:* skin detection model used, has lower percentage of detection.

Dnyanadajadhavand Prof.L.M.R.J.Lobo [2] -

Hand gesture recognition system to control slide show navigation.

***Disadvantage**:* Increase hassle because of hand markers

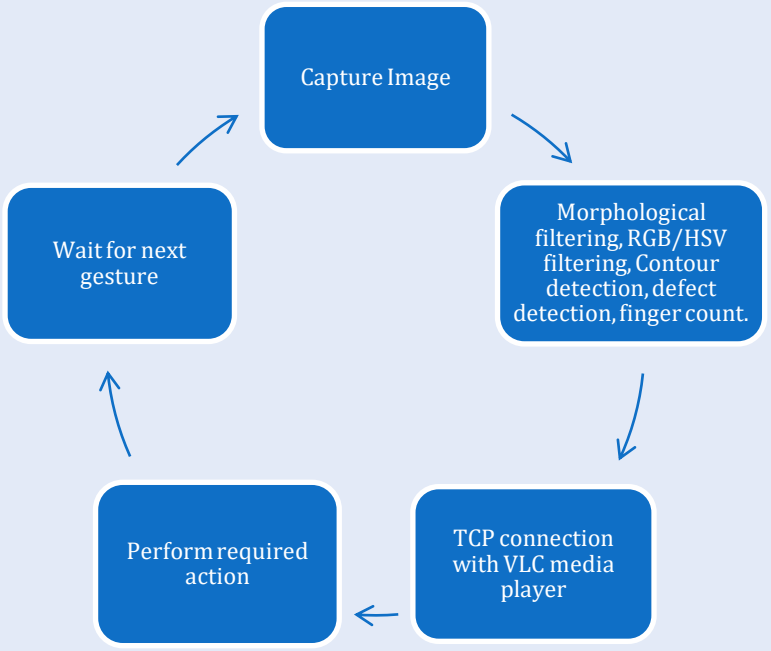
Advantage of proposed system:

Uses RGB/HSV filtering which has higher detection rate than above methods, also proposed system uses gloves for better recognition of hand, gloves are easily available as compared to hand markers.

PROPOSED SYSTEM

We have proposed a system solely based on java, as java is platform independent. Our system uses web-cameras which are acquitted in almost all laptops and are easily available for desktops. The input through a web-camera is accepted and recognized by our system to perform the desired action required by the user.

Architecture



METHODOLOGY

Web-camera provides a constant feed of inputs; this input is read one frame at a time to recognize the gesture made by the user. The input received is first filtered morphologically (see Figure 1)wherein the image of the user's hand is eroded (reduced to maximum visible area) for better recognition of individual fingers.

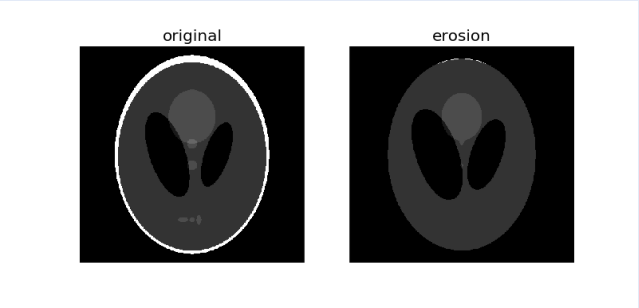


Figure 1: Morphological Filtering

After this step the morphologically filtered image is filtered using a rgb(Red, Blue, Green) range to detect only the elements with the specified color (the glove). [Figure 2.]

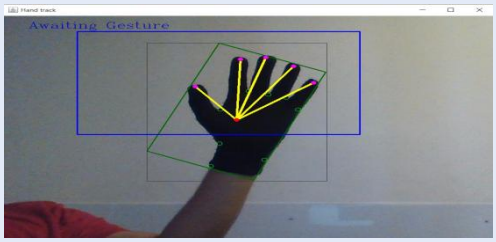
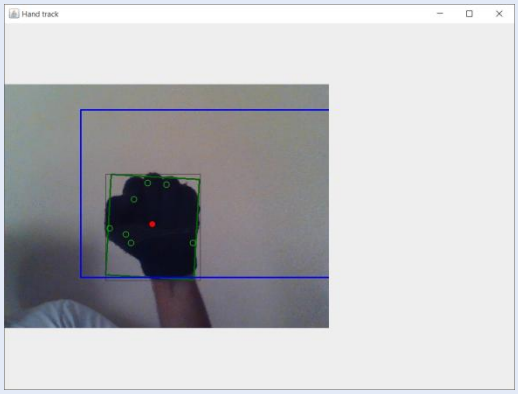


Figure 2: RGB Filtering Of Glove

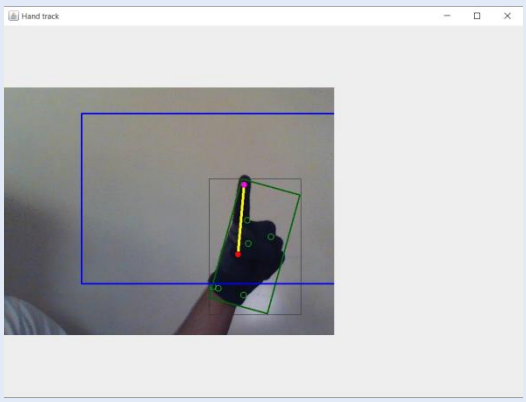
After this step the defects and contours are detected, the palm center is calculated and fingers are detected individually. After the detection of all the fingers the system waits for user to give command via gesture.

Following list of gesture commands are available with the system:



- Pause – 0 fingers (Clenched fists).

Figure 3: Zero (0) Fingers



- finger.

Figure 4: One Finger

- Volume Down (by 5 levels at a time) – Two fingers.

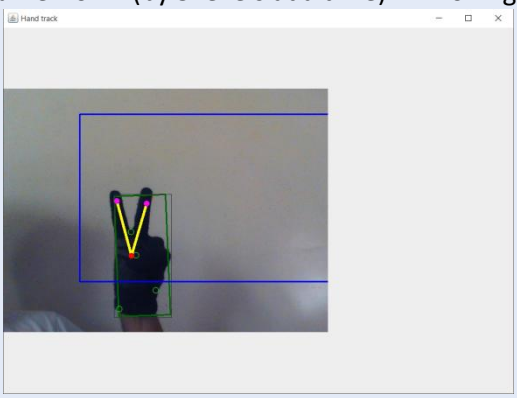


Figure 5: Two Fingers

- Next – Three fingers.

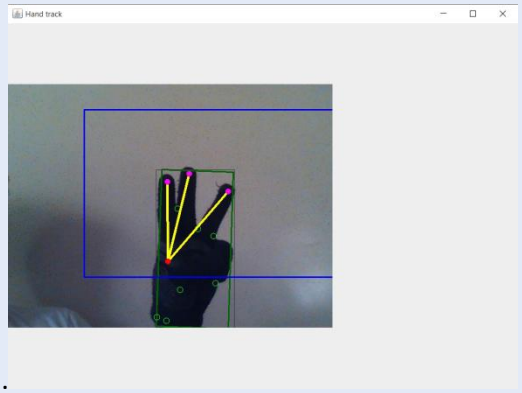


Figure 6: Three Finger

- Previous – Four fingers.

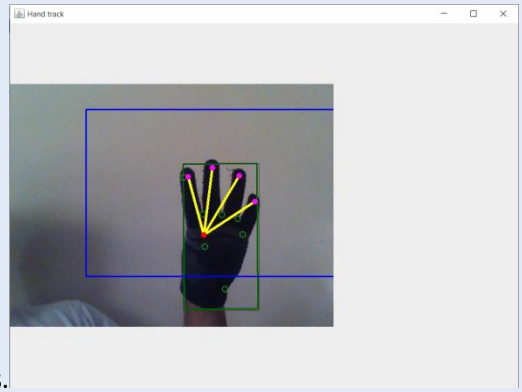


Figure 7: Four Fingers

- fingers.

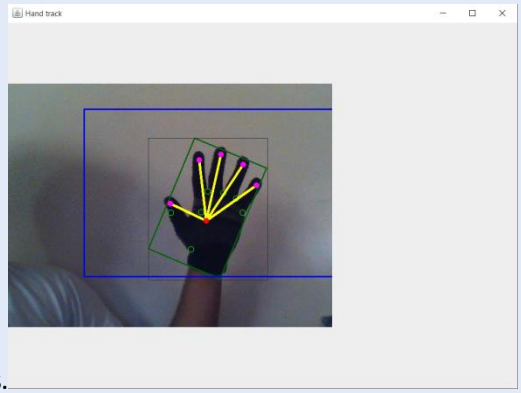


Figure 8: Five Fingers

PERFORMANCE

Performance of the system under ideal conditions is 98%. Ideal conditions defined as:

- Proper illumination of surroundings,
- No black color background (as system is tuned to detect black gloves),
- Black gloves (without pattern preferred).

Processing speed is dependent on the hardware configuration.

Minimum requirements:

- Dual core or up Processor (Clock speed 1.5Ghz).
- 1GB RAM.
- Onboard graphic processor.
- 100MB storage memory.

CONCLUSION

Basic VLC media player operations like play/pause, volume up/down, stop are made performable using gestures. The implementation of this system renders easy media viewing experience for users. Enables users to access the computer from a distance. Aids differently abled individuals to operate the computer without physical interaction. No additional hardware cost is required for laptops, for desktops web-cameras are available at a very low cost.

FUTURE WORK

The future scope of this system is to operate the mouse pointer with only gestures, thus enabling system wide access using gestures through the web-camera.

REFERENCES

1. Custom 3D Depth Sensing Prototype System for Gesture Control, http://www.gesturetek.com/3ddepth/introduction.php
2. Prime Sense, http://www.primesense.com/?p=488
3. NIPPON SYSTEMWARE's Gesture Recognition Software: DigiInfo, May 14th 2010. Retrieved from http://newtechs.net/2010/05/nippon-systemwares-gesture-recognition- software-diginfo/
4. N.KrishnaChaitannya and R.Janardhan Rao – Controlling of windows media player using hand recognition system.
5. DnyanadaJadhav and Prof.L.M.R.J. Lobo – Hand gesture recognition system to control slide-show navigation.

About the Authors:

Indrajeet Vadgama
vadgamaindrajeet@gmail.com

Yash Thaker
thakeryash20@gmail.com

Yash Khot
yashlee17@gmail.com

Pranali Jouras
pranalijouras@gmail.com

GREEN COMPUTING

Compiled by:

Jayalakshmi J nair and Nayana P V

ABSTRACT

Green computing is defined as the study and practice of designing , manufacturing, using, and disposing of computers, servers, and associated subsystems-such as monitors, printers, storage devices, and networking and communications systems-efficiently and effectively with minimal or no impact on the environment." The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Research continues into key areas such as making the use of computers as energy-efficient as possible, and designing algorithms and systems for efficiency-related computer technologies.

INTRODUCTION

A green computer or green IT system is one where the entire process from design, manufacture, use, and disposal involves as little environmental impact as possible. In other words, a green initiative is taken in consideration of all facets of a computer's life, from design to disposal.

In the design aspect, a green computer is created to perform without a negative environmental impact. Such design includes everything from materials and components to how the computer uses its power supply. Nowadays, most computers are built with a sleep or hibernate mode that allows them to power down when not in use and, therefore, save on energy impact.

A green computer will also take into account how it impacts the environment during its life. One way to make a green computer reduce its usage impact is to extend its longevity. The longer the computer lasts, the less impact it will have on the environment because disposal, normally the most significant green influence of the computer's cycle, will be delayed for a longer period of time. To increase a computer's longevity, we suggest looking toward upgrades and modularity. For example,

building a new computer from scratch produces a greater environmental effect than building a new RAM module for replacement in computing equipment.

computer virtualization is helping to make large strides .In green computing technology. Through the phenomenon of virtualization, it is now possible to operate two or more computers on the physical hardware of a single computer. In this manner, you could create the ultimate green computer; one that exists logically, but not physically. The logical units use all the material components of the physical computer, but are devoid of physical structure themselves. This means that the environmental impact of logical computers is virtually eliminated. The ideal green computer, therefore, may lie in virtual green computing.

Terminal servers can also be used to create a greener computer. When using a terminal server, you are connected to a central terminal where all the computing is done. The operating system is experienced by the end user on the terminal. These terminals can be matched up to thin clients who depend on the server to do most of their computing. This type of green computing setup typically consumes as little as one eighth of the energy of a conventional workstation.

Some of the world's leading companies that engage in green computing by researching green technology, developing energy efficient products, using sustainable materials, offering recycling programs, and marketing a greener look and feel, include well-known brands such as:

Nokia, Apple, Microsoft, Dell, Samsung, LG, IBM, Sony

One of the biggest challenges to successful green computing is disposal. Many computers contain harmful elements such as lead, mercury, and others. Safely recycling these computers has become of more and more concern in recent years. It is a good idea to consider donating your old PC to a charity or having it re-purposed for use in some other capacity.

BENEFITS OF GREEN COMPUTING

Cost savings

Better branding

Risk management

Resource utilization

Environment sustainability

Improved cooperate image

SHUT DOWN AND SWITCH OFF

Whilst putting a computer into a "standby" or "sleep" mode will save a lot of power, many people remain unaware that even shutting down a desktop computer completely does not turn it off. This is because the computer's power supply will remain physically switched on, with the motherboard partially powered and waiting for a signal from the switch on the front of the PC (which is not a mains power switch) to boot up again. To actually prevent a desktop computer from using power, after being shut down it must either be switched off at the wall socket, or turned off using the small rocker switch on the back of the power supply.

VIRTUALIZATION

Whilst the cost of computer processing power continues to fall, the cost of fuelling that processing capacity is rising. Energy costs indeed now exceed hardware costs over the lifetime of most business PCs, let alone servers. Corporate data centers have also been reported to be using about 1.5 per cent of the energy output of the United States. Any measure than can reduce the energy consumption of business computing is hence very welcome, and top-of-the-list in terms of the data centre is virtualization.

ENERGY EFFICIENT CODING

Whilst all of the above measures are intended to permit computers to most energy-efficiently run existing applications, an alternative approach to power saving is energy efficient coding. The principle behind energy efficient coding is to save power by getting software to make less use of the hardware, rather than continuing to run the same code on hardware that uses less power. Of course combining these two approaches can lead to even greater energy savings.

For many years, writing small and efficient -- let alone energy conscious -- software has hardly been a priority given continual increases in computer processor power and storage capacity. A great deal of "bloatware" is therefore now in existence. However, with some estimates suggesting that energy efficient coding could reduce the energy consumption of data centers by 25 to 30 per cent, it is unlikely to be possible to continue to ignore electricity usage as a factor in good software design.

COMPUTING AND SUSTAINABILITY

When it comes to being green, computing as both an industry and a broader human activity is unusual in that it may be both part of the problem and part of the solution. Indeed, as Intel highlighted in their excellent 2007 white paper on Advancing Global sustainability through technology, the microprocessor has the potential to become one of the "most energy-efficient, emission-reducing devices ever created".

There are three basic ways in which computer application can assist with reducing humanity's environmental impact. These comprise:

Increasing business efficiency

Dematerialization, and

Travel reduction

ADVANTAGES AND DISADVANTAGES OF GREEN COMPUTING

Reduced energy usage from green computing techniques translates into lower carbon dioxide emissions, stemming from a reduction in the fossil fuel used in power plants and transportation.

Conserving resources means less energy is required to produce, use, and dispose of products.

Saving energy and resources saves money.

Green computing even includes changing government policy to encourage recycling and lowering energy use by individuals and businesses.

Reduce the risk existing in the laptops such as chemical known to cause cancer, nerve damage and immune reactions in humans.

CONCLUSION

Whilst the performance and the breadth of application of computers is increasing, so too is our awareness of the cost and scarcity of the energy required to power them, as well as the materials needed to make them in the first place. However, because computing developments can enable individuals and businesses to adopt greener lifestyles and work styles, in terms of the environmental debate computing is definitely both part of the problem and part of the solution.

Through more environmentally aware usage (such as more effective power management and shut-down during periods of inactivity), and by adopting current lower power technologies, computers can already be made significantly more energy efficient. Indeed, just as we now look back and

wonder why automobiles a decade or two ago used to guzzle so much petrol, in a decade's time we will no doubt be staggered that a typical desktop PC used to happily sit around drawing 100-200W of power every hour night and day, and when accomplishing no more than displaying a screensaver.

The computing industry is more prepared and far more competent than almost any other industry when it does to facing and responding to rapid change. Environmentally it is not a good thing that most PCs -- especially in companies -- have typically entered a landfill after only a few years in service. However, this reality does at least mean that a widespread mindset already exits for both adapting to and paying money for new computer hardware on a regular basis. Hence, whereas it took decades to get more energy efficient cars on the roads, it will hopefully only take a matter of years to reach a state of affairs where most computers are using far less power than they needlessly waste today.

ACKNOWLEDGEMENT

We Jayalakshmi J Nair and Nayana P V take this opportunity to thank almighty God for making this presentation in proper manner. We also thankful to our Director U. Krishna Kumar sir , computer science faculty of Amrita School of Arts and Science for giving us such a wonderful opportunity. And finally we thank Computer Society of India for organizing such a great event.

About the Authors:

Jayalakshmi J nair

CSI:01333112

Nayana P V

CSI:01333129

GREEN TECHNOLOGY

Compiled by:

Preethi.R, V.Subedha and T.KalaiChelvi

INTRODCTION

Green technology is one of the innovative technology. Green technology conserve natural resource and the environment. It is environmental user friendly technology. Green technology is having some precious goals like rethinking, recycling, renewing, reducing, responsibility, energy, innovation, green building. Green computing, also called green technology, Green computing is the environmentally responsible use of computers and related resources. Green technology is important factor of growing awareness about environmental impact of computing. With rising global warming and electronic waste, energy consumption the idea of green computing is widely taken into serious consideration by both the government agencies and private companies.

GREEN TECHNOLOGY MERITS

Green technology merits are reduction in power and resource consumption, better resource utilization, improved operation efficiency and total cost(operational)savings.

GREEN TECHNOLOGY BARRIERS

Green technology barriers lack of motivation among stakeholders, lack of alignment between green IT and enterprise green initiatives ,fear of loss of job or need for retraining .

MODES

Two types of mode use to save energy while working on the computer such as sleep mode, hibernate mode. Sleep mode conserves energy by cutting off power to your display, hard drives and peripherals, hibernate mode saves energy by copying system data to reserved area on your hard disk. And the completely turned off your computer.

GREEN TECHNOLOGY APPLICATIONS

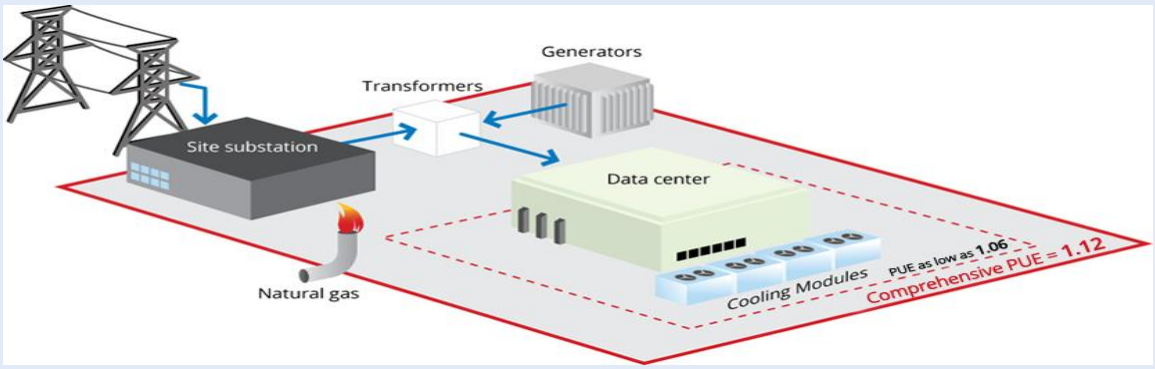
Green technology application are Electric Vehicles, Server Technology, Device Recycling and Server Technology

LATEST DEVELOPMENTS

DATA CENTER SUSTAINABILITY IMPROVEMENTS

Today's cloud providers to implement best practices to make datacenters operation green. Because they need The rising energy costs, desire to make existing investments more and more profitable. To build eco-friendly data center, several best practices in key areas has been proposed for improving sustainability:

1. Cooling system (new systems based on liquid cooling, nano-fluid cooling systems, and in-server, in-rack and in-row cooling by companies such as SprayCool; free cooling, spot cooling, using cable grommets to reduce cool air leakages).ICT platform (middleware-facility linkage, dedicated racks & servers, virtualization technologies).
2. Proper location which allows clean energy consumption through renewable sources .for example, wind power generating wind power, generating solar energy, cogeneration fuel cells.
3. Building design for example, optimizing floor layout, water recycling, heat insulation.
4. ICT platform (middleware-facility linkage, dedicated racks & servers, virtualization technologies).
5. Energy linking (power sharing between comp any centers, locating data center near power station).
6. Deployment of newest power efficient servers and processors
7. Energy linking for example, power sharing between company centers, locating data center near power station.



GREEN TECHNOLOGY OF FUTURE ENHANCEMENT

The increase in computing over the years has a direct impact on environmental issues and reducing the negative impact of computing on the environment is a main primary concern of future green technology.

REFERENCE

1. www.wikipedia.org

2. http://newtech.about.com/od/greencomputing/a/5-Applications- Of-Green-Technology.html

3. http://www.slideshare.net/neenasahni/green-computing- ppt

About the Authors:

R. Preethi is final year B.E Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. V. Subedha is Professor and Head of Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. T. Kalaichelvi is Professor ,Computer Science and Engineering at Panimalar Institute of Technology in Chennai, TamilNadu, INDIA.

HUMANOID ROBOT

Compiled by:

Steena Gracious and Shiby Sebastian

ABSTRACT

A HUMANOID ROBOT is a robot that is designed and developed such that its body shape resembles the human body. A humanoid design is the one which enable the functional purposes, such as interacting with human tools and environments , involving in researches and experiments, such as the study of bipedal locomotion. Besides the researches and experiments , humanoid robots are developed to perform human tasks like personal assistance , where they should be able to assist the sick and elderly , and dangerous jobs. They can be widely used for providing entertainment too. Humanoid robots are constructed in such a way that they imitate the human body. For achieving this, three primitives for robotics are Planning , sensor and control. The essential difference between a humanoid and other kind of robots lies within planning and control. Being one of the primitives of robotics , sensor plays the important role in robotic paradigms.

INTRODUCTION

A humanoid robot is a robot that is designed like its body shape resemble the human body. In general , a humanoid robot will look like a human being with a head, two arms ,and two legs and acts human behaviors and perform any human tasks like personal assistance and can involve in dangerous jobs. some forms of them may exhibit only part of the body. Androids are humanoid robots that are developed to aesthetically resemble humans beings . Another feature of humanoid robots is that they move, gather information on the "real world" and interact with it. They don't stay still like factory made other robots that

work in highly structured environments and have a predefined function. Humanoid robots are used as a research material in several scientific areas. They are becoming popular for providing entertainment too.

DESIGN GOALS

Humanoid robots are used as a research material in several scientific areas. Researchers need to understand the human behavior and body structure to build and study humanoid robots. On the other hand, the attempt to the facsimile of the human body leads to a better realizing of it. Human cognition is a branch of study that is focused on how humans learn from sensory information from its surroundings in order to acquire perceptual and motor skills. This knowledge will be helpful to develop computational models of human behavior and it has been improving over time.

Although the initial and fundamental aim of humanoid research was to build better orthosis and prosthesis for human beings , knowledge has been exchanged between both disciplines.

ADVANTAGES AND DISADVANTAGES

Besides the scientific researches, humanoid robots are being developed to perform human functions like personal support, where they should be able to assist the sick and elderly, and to do dirty or dangerous jobs. In essence, so long as they have the proper software , they can use machines and operate equipment in factories and vehicles designed for the human form, humanoids could theoretically perform any task a human being can. Humanoid robots with artificial intelligence , could be useful for future dangerous and distant projects like space exploration missions, without having the need to come back again to Earth once the mission is completed.

However, the complexity of doing day to day activities and complex tasks with such robots are deceptively great. Other major problem about humanoid robots is that they will replace jobs. it would affect those who have jobs in certain fields, such as pharmacists, mechanics , secretaries, etc. As humanoid robots becoming more and more popular in society ,Another disadvantage could be the price, depending on how advanced the robot is.

CONCLUSION

The humanoid research is a new approach in robotics to understand and realize the complex physical world interactions between a robot, an environment, and a human. Today we use different robots in many fields such as factories, warehouses, and laboratories. Robots are useful in many ways in our real world.

ACKNOWLEDGEMENT

If words are conceded as symbols of approval and tokens of acknowledgements, then words play the heralding role of expressing our gratitude .We would like to thank our teachers who guide us by giving valuable suggestions and priceless help given to us

REFERENCE

[1] Russell, S. J. & Norvig, P. (1995). Artificial Intelligence: A Modern Approach. Prentice- Hall. Prentice Hall.

[2] Everett, H. R. (1995). Sensors for Mobile Robots: Theory and Application. AK Peters. ISBN 1-56881-048-2.

[3]Arkin, Ronald C. (1998). Behavior-Based Robotics. MIT Press. ISBN 0-262-01165-4.

About the Authors:

Steena Gracious

steenagracious@gmail.com

CSI:01295351

Shiby Sebasian

shibysebasian96@gmail.com

CSI:01295348

CONNECTING INDIA THROUGH LI-FI TECHNOLOGY

Compiled by:

Gayathri P.M and Krishendu R Nair

ABSTRACT

We use Light Emitting Diodes (LED) in different areas of everyday life. This paper points out the usage of LED technology for wireless communication, which can be termed as LI-FI (Light Fidelity). LIFI is a new technology but it is no longer an idea, now it has emerged as a proven technology. This paper gives an idea about the advantages, disadvantages, applications and working of LIFI for transferring data from one computer to another. LIFI is a proven technology that can solve many drawbacks of the WIFI technology. New researches has been made on this technology to use visible.

INTRODUCTION

Nowadays the usage of internet increases through wired and wireless network. The uses increases automatically the speed become reduced. It is one of the major problems affected by the use in the busy world. Most of the people are using Wi-Fi technology to access the internet. It has an average speed of 150mbps, which is not sufficient to automate number of desired users. To remedy this problem a German Physict Harald Hass come up with a solution called Li-Fi (light fidelity). Capabilities of the existing Wi-Fi can be increased using Li-Fi technology. Li-Fi transmit data with the help of an LED bulb having high speed actually faster than human eye can follow. It is also known as usable light communication. This transfer of data is done through fiber out of fiber optics and sending data through LED light. Li-Fi provides high efficiency, large bandwidth, good security and more availability with a very high speed. In other words Li-Fi is the optical version of WIFI. By the use of LI-FI technology we can save large amount of electricity since data is transmitted through light bulbs. LIFI works based on a simple principle using LED that is if LED is ON ,then it transmits digital 1 .On the other hand if the LED is off then digital 0 is transmitted.

Figure. 1: Li-Fi bulb [1]

We can use Li-Fi wherever Wi-Fi is used. Li-Fi requires light for its working. .Since Li-Fi is a light based technology. There are mainly four criteria to identify the working of Li-Fi and Wi-Fi, it includes Security, efficiency, availability and capacity .Electromagnetic spectrum is used for transmission of

data in both Li-Fi and Wi-Fi. In the case of Wi-Fi it uses radio waves on the other hand Li-Fi uses visible light for communication. In this paper we discuss about comparison of Wi-Fi and Li-Fi and the paper also discuss about the working of Li-Fi and its applications.

WORKING OF LI-FI

We can implement the Li-Fi using white LED bulb at downlink transmitter. By varying the speed of the current at high speed we get the optical output at very high speed. This white LED bulb is fitted with overhead lamp using processing technology streams; we can use high speed data diode to embed the data. Then a receiver named dongle helps to change these variations to an electrical signal. Then it is converted back to data stream and transmitted to our devices [2].

ADVANTAGES OF LI-FI

The problem of less frequency and bandwidth can be solved using the Li-Fi technology. In Li-Fi the data transmission can be upto 10Gbps.Li-Fi provides more security than that of Wi-Fi, because light cannot penetrate through solid objects like walls. Maintenance cost is very low. Li-Fi is more safe for human body because light don't penetrate into the human body.

DISADVANTAGE LI-FI:

The major disadvantage is that it cannot pass through solids. The major problem was that how the receiving device will transmit the data back to the transmitter. Installation cost of the VHC system is high. One drawback of Li-Fi is that it gets inter faced by natural phenomenon.

COMPARISON OF LI-FI AND WI-FI

BASIC COMPONENT	WIFI	LIFI
Security	Not secured	Secured
Data Transmission Rate	Slower	Faster
Range	Small	Large
Traffic Control	Less	More
Working Concept	Various topologies	Direct binary data serving
Cost	Costly	Cheap

APPLICATION OF LI-FI:

We can implement Li-Fi in our day to day life in different fields like: Education System, Medical applications, and usage of internet in aircraft, under applications, disaster management, safety and management system, health sector, application in sensitive areas and mostly in using internet anywhere. Li-Fi can also be used in traffic signals, by using LI-Fi in traffic signals we can easily

communicate with LED lights and reduce the occurrence of accidents. In airlines Li-Fi can be used for data transmission .Petroleum and chemical plants works based on the Li-Fi technology, where other type of transmissions like radio transmission can hazardous[3].

CONCLUSION

Li-Fi is a developing technology and it has got vast potentials .The areas of application of Li-Fi are yet to be explored. Now Li-Fi has become a major technology of tomorrow .If efficiently used we can soon implement a technology that is same as that of Wi-Fi hotspots with just the availability of light bulb. It does not affect human and nature in any manner .So it is a safer technology .Using of Li-Fi technology can benefit the economic sector, because surveys points out that Li-Fi market will reach about $6 billion by 2018.It is a currently attracting technology since it acts as efficient and effective replacement for radio based wireless systems. Li-Fi helps to solve many drawbacks of radio technology .This technology can be implemented only in the presence of light. In general Li-Fi is a new technology for communication and has numerous possibilities and can be explored in the near future.

REFERENCES

1. http://www.dvice.com/archives/2012/08/lifi-ten-ways-i.php
2. Fernado,n, Long,g, and, viterbo,e,"flip-ofdm for optical wireless communication ,"[information theory workshop(itw)]15-9,ieee,[array ,brazil(oct-16-2011)
3. Amstronng and lowary . a" a power efficient optical ofd ofdm," Electronics letter 42,370-372(mar 16,2006).

About the Authors:

Ms. Gayathri P. M.
gayathripm96@gmail.com
CSI: 01295329

Ms. Krishnendu R. Nair
krishnendu96r@gmail.com
CSI: 01295334

Guided by,

Mr. Hari Narayanan A.G
Asst. Prof. of Computer Science department
Amrita school of Arts and Science, Kochi
Amrita Vishwa Vidhyapeetha

FIRE DETECTION THROUGH IMAGE ANALYSIS

Compiled by:

Rachana Tripathi, Ruchita Thakur and Sadhana Inchanale

ABSTRACT

Detecting the presence of fire in an image or video is one of the domain problems in computer vision. Visual based fire detection occurs to overcome the weakness of the conventional, especially in monitoring area. There has been a lot of proposed method to detect the presence of fire in image or video. Based on proposed method, the process to detect presence of fire in image or video can be considered as multi-filtering process. One of the phase for fire detection is to determine candidate fire based on their color. In this research we focus on determining the presence of fire in image based on their pixel intensity and their distribution. Fire has unique color that can be used to distinguish them from other objects. In this paper, novel models for fire and smoke detection using image processing is provided. The models use different colour models for both fire and smoke. The color models are extracted using a statistical analysis of samples extracted from different type of video sequences and images. The extracted models can be used in complete fire/smoke detection system which combines color information with motion analysis.

INTRODUCTION

Due to the rapid developments in digital camera technology and developments in content based video processing, more and more vision based fire detection systems are introduced. Vision based systems generally make use of three characteristic features of fire: color, motion and geometry. The color Information is used as a pre-processing step in the detection of possible fire . There are lots of fire detection systems in which the color information is used as a pre-processing step. Phillips et al. used color predicate information and the temporal variation of a small subset of images to recognize fire in video sequences . A manually segmented fire set is used to train a system that recognizes fire like color pixels. The training set is used to form a look-up table for the fire detection system. The authors offer the use of generic look-up table if the training set is not available. Chen et al. used chromatic and Dynamic features to extract real fire and smoke in video sequences. They employ a moving object detection algorithm in the pre-processing phase. The moving objects are filtered with fire and smoke filter to raise an alarm for possible fire in video. They used a generic fire and smoke model to construct the corresponding filter. Töreyin et al. proposed a real-time algorithm for fire detection in video sequences

They combined motion and color clues with fire flicker analysis on wavelet domain to detect fire. They have used a mixture of ten three dimensional Gaussians in RGB color space to model a fire pixel using a training set. Töreyin et al. proposed another algorithm for fire detection which combines generic color model based on RGB color space, motion information and Markov process enhanced fire flicker analysis to create an overall fire detection system they have employed the fire color model developed by Chen et al. Later on they have employed the same fire detection strategy to detect possible smoke samples which is used as early alarm for fire detection. They combined color information with shape analysis to detect possible smoke samples where false alarm rate is decreased using a flicker analysis of smoke region.

Recently, Celik et al. proposed a generic model for fire color. The authors combined their model with
Simple moving object detection. The objects are identified by the background subtraction technique. Later on they have proposed a fuzzy logic enhanced approach which uses predominantly luminance information to replace the existing heuristic rules which are used in detection of fire-pixels. YCbCr color space is used rather than other color spaces because of its ability to distinguish luminance from chrominance information. The implicit fuzziness or uncertainties in the rules obtained from repeated experiments and the impreciseness of the output decision is encoded in a fuzzy representation that is expressed in linguistic terms. The single output decision quantity is used to give a better likelihood that a pixel is a fire pixel. The fuzzy model achieves better discrimination between fire and fire like-colored objects. Since the color based pre-processing is essential part for all image processing based fire and smoke detection systems, an efficient color model is needed. In this paper, we have further improved the model defined in our previous work to detect fire pixels using fuzzy logic and proposed a model for smoke-pixel detection. The proposed color model for fire detection is compared with the existing techniques.

NEED AND UPDATION TO SYSTEM

NEED FOR SYSTEM

Current system of fire or smoke detection use electronic sensors which use radiation heat to detect smoke or fire by detecting change in temperature. In such system the main drawback is sensors can't cover outdoor area or large area such as forests, petrochemical refineries, saw mills etc. where we can't install sensors over a large area. Installing electronic sensors is not feasible in such locations. Secondly, the other drawback is of time, heat radiation or smoke should reach sensor before sensor can detect it. Vision based fire detection is potentially a useful technique. With the increase in the number of surveillance cameras being installed, a vision based fire detection capability can be incorporated in existing surveillance systems at relatively low additional cost.
Vision based fire detection offers advantages over the traditional methods. It will thus complement the existing devices. Each fire detection method is better suited to a distinct environment. Vision based fire detection has the following advantages over the other methods. First, it has fast response to fires. Like the radiation based method, it detects fires as soon as they appear in sight. Second, it directly senses the location of fire (in 2-D), not just radiation which comes from its general vicinity. Last, but not least, it is capable of analyzing existing images or image sequences so that it can be used for
Multimedia database retrieval. Line of sight visual methods like this complement other methods that use associated cues of smoke and heat.
Hence this approach of fire and smoke detection is very helpful in outdoor locations which cover large area and where it is not feasible to put electronic sensors.

UPDATES IN CURRENT SYSTEM

When a fire occurs, minimum detection latency is crucial to minimizing damage and saving lives. Current smoke sensors inherently suffer from the transport delay of the smoke from the fire to the sensor. A video smoke detection system would not have this delay. Further, video is a volume sensor, not a point sensor. A point sensor looks at a point in space. That point may not be affected

by smoke or fire, so the smoke would not be detected. A volume sensor potentially monitors a larger area and has much higher probability of successful early detection of smoke or flame.
Video smoke detection is a good option when smoke does not propagate in a “normal” manner, e.g., in tunnels, mines, and other areas with forced ventilation, and in areas with air stratification, e.g., hangars, warehouses, etc. Video is also a good option for large, open areas where there may be no heat or smoke propagation to a fixed point, e.g., saw mills, petrochemical refineries, forest fires, etc.

CONCEPT AND EVALUATION

CONCEPT

1. PURPOSE
Current system of fire or smoke detection use electronic sensors which use radiation heat to detect smoke or fire by detecting change in temperature. In such system the main drawback is sensors can’t cover outdoor area or large area such as forests, petrochemical refineries, saw mills etc. where we can’t install sensors over a large area. Installing electronic sensors is not feasible in such locations. Secondly, the other drawback is of time, heat radiation or smoke should reach sensor before sensor can detect it. Vision based fire detection is potentially a useful technique. With the increase in the number of surveillance cameras being installed, a vision based fire detection capability can be incorporated in existing surveillance systems at relatively low additional cost.

2. PRODUCT SCOPE
The system can be used for surveillance the wide spread areas where the chance or probability of catching fire is more (e.g. :-Forest , Saw mill , Petrochemical industries etc.). Besides detecting fire it can also be used for surveillance large areas, we just need to install webcam in proper place. System can further be used in satellites for detecting fire from satellite image.

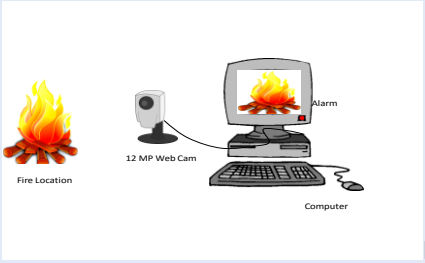
3. REFERENCES
IEEE paper

4. OVERVIEW
Requirements specification is organized in two major sections – Overall descriptions and Specific requirements .The first section describes the general factors that affect the product and its requirements. This section does not state specific requirements. Instead, it provides a background for requirements. This section of the SRS contains all of the software requirements to a level of detail sufficient to enable designers to design a system to satisfy those requirements, and testers to test that the system satisfies those requirements.

5. OVERALL DESCRIPTION
The software requirement specification is produced at the culmination of the analysis task. the performance allocation to software as part of the system engineering are establishing a complete information description, a detailed functional and behavioral description, an indication of performance requirements and design constraints, appropriate validation criteria and other data pertinent to requirement. User fixes the camera at a location from where the camera captures the surveillance area. Background processing such as taking frames from the video and subtracting frames from the video. Convert the RGB image of frames into bitmap image. Make three clones of

this bitmap image. Convert clones into Y, Cb, Cr color space respectively. We can compare the difference of (Y-Cb & Cr-Cb) for fire pixel and for non-fire pixel.
As this difference is greater in fire pixel then non-fire pixel, we can detect fire in the frame.

6. PROTOTYPE



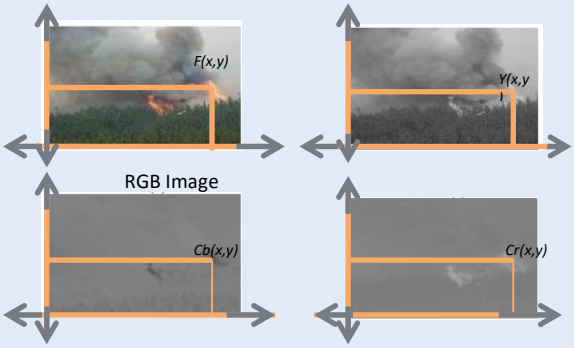
Framework for recommended system contains various modules. Each module work independently. Each module take the video from camera and convert it into frames, each frame is then converted to bitmap image and here we take three clones of this bitmap image, each clone is then converted to Y, Cb, Cr channel respectively with help of equations given below.

$Y = 0.299R + 0.587G + 0.114B$

$Cb = -0.169R - 0.331G + 0.500B + 128$

$Cr = 0.500R - 0.419G - 0.082B - 128$

Then we take the difference of Y-Cb and Cr-Cb, as for fire pixel Y-Cb and Cr-Cb is greater than non-fire pixel.



7. EXTERNAL INTERFACE REQUIREMENTS

The external interfaces requirements provide a description of all inputs and outputs associated with the framework of Fire detection software.

8. USER INTERFACES

The user interface is the mean of communication between the user and the software system. It has to be simple and easy to use and learn.

9. SOFTWARE INTERFACES

The software interfaces are nothing but the flow of screens of forms that are occurring one after the other when user is using the system.

10. SYSTEM FEATURES

The Fire and Smoke detection software has a well-designed and user friendly GUI.
It uses less number of cameras for area surveillance.
It is helpful in early fire detection.
It works on special characteristics of fire and smoke in YCbCr and HSL color space.

Detection rate is much faster than usual electronic sensors.

IMPLEMENTATION

1. AForge.NET Framework

AForge.NET Framework is a C# framework designed for developers and researchers in the fields of Computer Vision and Artificial Intelligence - image processing, computer vision, neural networks, genetic algorithms, machine learning, etc.

2. Aforge.imaging.filters

The AForge.Imaging.Filters namespace contains collection of interfaces and classes, which provide different image processing filters. Classes of this namespace allow to do different transformation of a source image, doing it directly on the source image or providing new image as a result of image processing routine.

3. YCbCr filtering

Framework for recommended system contains various modules. Each module work independently. Each module take the video from camera and convert it into frames, each frame is then converted to bitmap image and here we take three clones of this bitmap image, each clone is then converted to Y,Cb,Cr channel respectively with help of equations given below.

$Y = 0.299R + 0.587G + 0.114B$

$Cb = -0.169R - 0.331G + 0.500B + 128$

$Cr = 0.500R - 0.419G - 0.082B - 128$

Then we take the difference of Y-Cb and Cr-Cb, as for fire pixel Y-Cb and Cr-Cb is greater than non-fire pixel.

4. HSL Filtering

For smoke detection below given equation should be satisfy

$|R(x, y)-G(x, y)| < Th$

$|G(x, y)-B(x, y)| < Th$

$|R(x, y)-G(x, y)| < Th$

Where Th is a global threshold ranging from 15 to 25.

EVALUATION

Framework for recommended system contains various modules. Each module work independently. Each module take the video from camera and convert it into frames, each frame is then converted to bitmap image and here we take three clones of this bitmap image, each clone is then converted to Y,Cb,Cr channel respectively with help of equations given below.

$$Y = 0.299R + 0.587G + 0.114B$$

$$Cb = -0.169R - 0.331G + 0.500B + 128$$

$$Cr = 0.500R - 0.419G - 0.082B - 128$$

Then we take the difference of Y-Cb and Cr-Cb, as for fire pixel Y-Cb and Cr-Cb is greater than non-fire pixel.

For smoke detection below given equation should be satisfy
|R(x, y)-G(x, y)| <Th
|G(x, y)-B(x,y)|<Th
|R(x, y)-G(x, y)|<Th
Where Th is a global threshold ranging from 15 to 25.

TESTING

Testing strategy followed:
The spiral model for testing is followed which includes following phase:
Unit testing
Integration testing
Validation testing
System testing

UNIT TESTING

Under unit testing, with the use of white-box testing technique, each component or module is tested individually, to ensure that it works properly.

- Local data structure is examined for each module, which ensured that data stored maintains its integrity during all steps in an algorithms execution.
- Boundary conditions are checked for each module, which ensured that module operates properly at boundaries.
- All independent paths are through the control structure are examined which ensured that all statements have been executed at least once.
- All error handling paths are tested.

VIDEO PROCESSING:

Input test case	Expected Output	Actual Output
To check whether the s\w convert the video into frames.	7 to 10 frames per second	As expected
Does the filter convert each frames into respective Y,Cb,Cr color space for fire detection.	Filter should convert each frame into Y,Cb,Cr color space.	As expected
Does filter	Yes	As expected

convert each frame	converted	

Fire Detection:

Input test case	Expected Output	Actual Output
To check whether s\w detect all the fire samples in the day conditions.	All the fire samples should be detected.	As expected
To check whether s\w detect all the fire samples in the night conditions.	All the fire samples should be detected.	As expected
To check whether s\w detect bright color object.	Bright color object except fire should not be detected.	As expected

Smoke detection:

Input test case	Expected Output	Actual Output
To check whether s\w detect all the smoke samples in the day conditions.	All the smoke samples should be detected.	As expected
To check whether s\w detect all the smoke samples in the night conditions.	All the smoke samples should be detected.	As expected

Filter Operations:

Input test case	Expected Output	Actual Output
To check whether each frame has came to YCC and HSV filter.	Each frame should be come into the filter for processing.	As expected
To Check whether each frame has converted to respective Y,Cb,Cr channels.	Each frame should be converted into Y, Cb, Cr channel.	As expected
To Check whether each frame has	Each frame should be converted into	As expected

converted to HSV channels.	HSV channel.	

INTEGRATION TESTING

Input test case	Expected Output	Actual Output
To check whether each frame is processed by YCC and HSV filter	Each frame should be processed by YCC and HSV filter.	As expected
To check whether the module for smoke detection detect smoke in the frame	Modules should detect smoke instantly.	As expected

SYSTEM TESTING

Input test case	Expected Output	Actual Output
To check whether the Fire and smoke detection s\w is functional on all the OS	Fire and smoke detections\w should be functional on other OS	As expected

TEST RESULTS

There are separate modules each for administrator and user. And the front end of the each has to be tested for the prompt error handling and the correct outputs. Every module has proper generation of messages which help the user and the administrator to follow proper path of the system. Tests are implemented in case of each possible condition.

In login module the testing is done by giving various inputs in the textboxes “User name and passwords”. During the simulation of this module it has been tested whether the error messages are displayed at the needed point for e.g. if a wrong type username or password is given the system should generate error messages.

CONCLUSION

This system can be used in detecting fire in locations like Forest, Petrochemical Industries,and Saw Mill which cover large area and it is not possible to put sensors everywhere. This can further be modified to detect fog, measuring visibility distance etc.
Hence we can conclude that our software for fire and smoke detection by image processing has an edge over our usual electronic sensors

ACKNOWLEGEMENT

Authors are thankful to Mr. Manish Salvi for his guidance in completion of the project and his valuable guidance.

REFERENCES

1. Celik, T., Demirel, H., Ozkaramanli, H., Uyguroglu, M., “Fire Detection in Video Sequences Using Statistical Color Model” *Proc. Internat. Conf. on Acoustics, Speech, and Signal Processing*, vol. 2, no.pp. II-213 - II-216, May 2006.
2. Celik, T., Demirel, H., Ozkaramanli, H.,”Automatic Fire De-tection in Video Sequences”, *European Signal Processing Conference*, EUSIPCO-06, Sept. 2006.
3. Chen, T., Wu, P., Chiou, Y.,”An early fire-detection method based on image processing”, *Proc. IEEE Internat. Conf. on Image Processing*, ICIP’04, pp. 1707-1710, 2004.
4. Klir, G. J., Yuan B., *Fuzzy Sets and Fuzzy Logic* , Prentice Hall, 1995.
5. Mathews, J.H., Fink, K.D., *Numerical Methods using MATLAB* , Prentice Hall, 1999.
6. Phillips III, W., Shah, M., Lobo, N.V,:”Flame recognition in video”, Pattern Recognition Lett. 23 (1–3), 319–327, 2002.
7. Töreyin, B.U., Dedeoglu, Y., Güdükbay, U., Çetin, A.E, “Computer vision based method for real-time fire and flame detection”, *Pattern Recognition Lett.* , 27 (1-1), 49-58, 2006.
8. Töreyin, B.U., Dedeoglu, Y., Çetin, A.E.,”Flame detection in video using hidden Markov models”, *Proc. IEEE Internat. Conf. on Image Processing* , pp. 1230-1233, 2005.
9. Töreyin, B.U., Dedeoglu, Y., Çetin, A.E.,” CONTOUR BASED SMOKE DETECTION IN VIDEO USINGWAVELETS ”, *European Signal Processing Conference* , EUSIPCO-06, Sept. 2006.
10. Turgay Celik, Huseyin Ozkaramanli, Hasan Demirel,” FIRE PIXEL CLASSIFICATION USING FUZZY LOGIC AND STATISTICAL COLOR MODEL”, *ICASSP 2007*.

About the Authors:

Ms. Rachana Tripathi, Student, Mumbai University

Ms. Ruchita Thakur, Student, Mumbai University

Ms. Sadhana Inchanale, Student, Mumbai University

TRAVELYAN:TRAVEL BUDDY

Compiled by:

Karan Thakkar, Sanket Kamath, Romil Shah and Chirag Gawde

ABSTRACT

Travelyan is an application which has the potential to become the social hub for people who love to travel. Users can search for planed trips as well as user experiences, tips, advice, etc. and plan a perfect travel without help of any travel agent without spending any money for planning their trip. Never miss an attraction, just because you weren't informed about it.

INTRODUCTION

The application is a mobile application that's provide services to browse, trace &navigate a route on a Map as well as see locations of other users who allow it using their GPS. Travelyan is implemented using Google® Android platform which is a software stack for mobile devices including operation system, middleware and other key application. It uses maps API of OpenStreetMap (OSM) "©OpenStreetMap contributors". Travelyan will allow everyone to see and follow directions to a destination. Using this application, users can plan their vacation trips and save it for others to follow. It is mainly focused on users who want to plan their own trips without any help from Tour Travel Agencies. Users will be provided links to blogs and related information about a certain place. If the app is used for trips and treks, user can share their GPS locations and see each other's location in real time. Users can directly see someone else plan of trip and use it to plan their own taking their tips in mind. The application will help the users to plan all kinds of trips, especially for users in large groups in such a way that it will be easier for the users to plan their trips efficiently.

Working

The user of Travelyan is everyone who has mobile device, such as mobile phone, smart phone or personal digital assistance (PDA), which runs under Android platform. A social account to link the user account with & Internet for planning, exploring, etc. Users can be divided into two major classes.

Trip Planners - This class of user will plan the entire trip and save it for others to follow. These are the actual itinerary creators who can make changes to further plans according to the advice of people who have already followed it.

Trip Members - This class of users will use the planned trips as their itinerary and follow the plan set by the planner for their excellent trip.

The application will be implemented, tested, and integrated on Android platform. The platform provides an operating system, middle ware, core features, and API that allow access to perform activity on mobile device system. Internet connection of smart phone is also required.

IMPLEMENTATION AND METHODOLOGY

The application design primarily depends on Google® Android architecture using its -

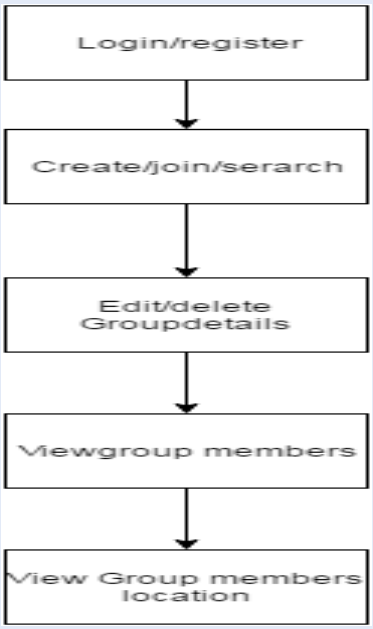
API-Its user interface for smart phones is written with Java (Android Studio)

All code shall use Sun® Java programming language.

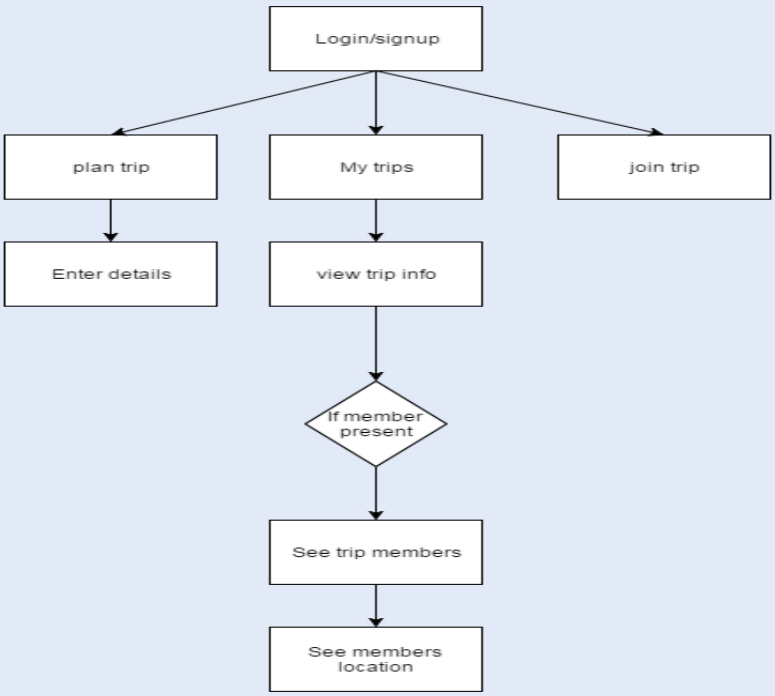
A user document will be prepared after the application is designed completely so that it will act as a user help manual when the user wants to use the application.The user interface of the application will enable the user to interact with application. The application will take the user input via the keypad of the mobile phone device and make the necessary changes or additions desired by the user. The user will be able to see these additions via the device screen. The application provides a graphical user interface to the users which depict various features of the application like trip planner, maps, etc.

The application uses services of mobile device's operating system through API provided by Android.OSM API uses REST web service interface for reading and writing to the database i.e. XML over HTTP, with use of simple URLs for object access, and standard HTTP response codes. The help button will allow the user to select certain contacts which will receive an alert about the user location if the user is in trouble. The application will allow the user to locate the exact locations of the user's friends and group members when on trips. This feature is basically a GPS driven location feature. User enables GPS on the mobile phone. The location finder GPS then finds location of the user's friends and group members. The application will give the users suggestions on nearby points of interests in their vicinity and also show up reviews to the locations from other tourists and travel enthusiasts. User enables GPS on the mobile phone. The location finder GPS then finds places of interests and reviews of locations. The application will allow the user to know the last known exact location of a group member using the application. User enables GPS on the mobile phone. The location finder GPS then finds and notifies other users about the last known location of a particular user or group member. Travelyan is an application that requires certain system resources to carry out its basic functions. The app will use these system functions in such a way that it won't delay the system from performing other key processes in any way. The program response time is direct and it will have a real time response. The application will not use any of the information provided by the user for any other purpose except for the trip planning and other feature driven purposes. All the data of the users will be confidential and will not be disclosed to anyone. The application will help users when the user gets stuck on a certain activity with the help of tips and suggestions. Information given by users at the registration page is kept in the system database. This information cannot be reached by other users or external threats. The users in the application are all equal so there is not the need of any identity management level. This application provides a pleasant and user friendly graphical interface with relatively simple functions. Any user should be able to use Travelyan without any specific knowledge or experience. The user must only input some of the basic information that is needed so that the application can be used to its full potential.

BLOCK DIAGRAM



FLOW CHART



EXISTING SYSTEM

Major applications like Trivago, Make My Trip and Yatra are applications similar to Travelyan. These applications basically are used to carry out and plan trips to locations. These applications offer customers various features such as trip fare comparisons, budget settings and reviews of destinations along with offers for trips. Travelyan is based on an idea similar to the domain of

tourism, but goes in a completely different and unchartered territory when it comes to travelling applications.

PROPOSED SYSTEM

The user interface of the application will enable the user to interact with application. The application will take the user input via the keypad of the mobile phone device and make the

Necessary changes or additions desired by the user. The user will be able to see these additions via the device screen. The application provides a graphical user interface to the users which depict various features of the application like trip planner, maps, etc. Travelyan will allow everyone to see and follow directions to a destination. Using this application, users can plan their vacation trips and save it for others to follow. It is mainly focused on users who want to plan their own trips without any help from Tour Travel Agencies. Users will be provided links to blogs and related information about a certain place. If the app is used for trips and treks user can share their GPS locations and see each other's location in real time. Users can directly see someone else plan of trip and use it to plan their own taking their tips in mind. The application will help the users to plan all kinds of trips, especially for users in large groups in such a way that it will be easier for the users to plan their trips efficiently.

The application provides several features:

Offline Maps

Plotted path with markers

Checkpoints

Places of interests

GPS refresh rate

Timely Notifications

Location of other members

Day wise trip planner

Help button

Social Login

Blog's & Link Related to a place Review

FUTURE WORK

Offline Maps - The application will allow the user to take the map offline so that he can use it for navigation even without an active internet connection.

ACKNOWLEDGMENT

We would like to thank our guide Prof. Joel Philip, Lecturer at Universal College of Engineering for his guidance and support. We will forever remain grateful for the constant support and guidance extended by guide, for the completion of paper.

REFERENCES

1. Mobile Tracking Application for Locating Friends using LBS Abhijeet Tekawade, Ahemad Tutake, Ravindra Shinde, Pranay Dhole - U.G. Students, Dept. of Computer Engineering, KJ College of Engineering and Management Research, Pune, India, Mr. Sumit Hirve - Assistant Professor, Dept. of Computer Engineering, KJ College of Engineering and Management Research, Pune, India.
2. Implementation of Location based Services in Android 237 Copyright (c) 2012 International Journal of Computer Science using GPS and Web Services ABV-Indian Institute of Information Technology and Management Manav Singhal, Anupam Shukla ABV-Indian Institute of Information Technology and Management Gwalior, India.
3. Location Based Services and Integration of Google Maps in Android by Pankti Doshi – Assistant Professor - NMIMS University, Pooja Jain, Abhishek Shakwala - NMIMS University, Assistant Professor, Department of Computer Engineering, NMIMS University, Mukesh Patel School of Technology Management and Engineering, V.L. Mehta Road, Vile Parle (W), Mumbai – 400056.
4. Position Detection and Tracking System - Mahesh Kadibagil - PG Scholar, Dept. of ISE, BMSCE, Bangalore, India and Dr. H S Guruprasad Professor and Head, Dept. of CSE, BMSCE, Bangalore, India.
5. GEO ALERT- A Location Based Alarm System Using GPS in Android Deepika Garg - Jayoti Vidyapeeth Women's University, Jaipur, India, Dr. Anupam Shukla - ABV-IIITM, Gwalior, India.

About the Authors:

Mr. Karan Thakkar, Mr. Sanket Kamath, Mr. Romil Shah and Mr. Chirag Gawde
karan.d.thakkar@gmail.com , kamath.sanket4@gmail.com, sromil7@gmail.com, gawdechirag70@gmail.com
Information Technology
Universal College of Engineering, Kaman, Vasai (East), Thane, Maharashtra, India

ATTENDANCE MONITORING SYSTEM (AMS) USING RFID CARD TAPPING AND FACE RECOGNITION TECHNIQUE

Compiled by:

Prashant Prajapati, Sejal Patel and Prathamesh Sadekar

ABSTRACT

Employee management, today, is widely practiced in all workplaces. Day by day security breaches and transaction fraud increases, the necessity for secure identification and private verification technologies is turning into a good concern to the organization. Therefore, efficient management of attendance is to be established. The system will include following methods of attendance monitoring:

Biometric Face Recognition

RFID smartcards

These two techniques are used for developing an advanced and secure system. Human face recognition is an important branch of biometric verification and has been widely used in many applications, such as video monitor system, human-computer interaction and network security. RFID Technology is also used for managing the attendance monitoring system. The system can record the group action of the staff within the organization surroundings and it'll offer the facilities to the admin to access the knowledge of the staff simply by maintaining a log.

INTRODUCTION

The goal of the project is to develop an integrated attendance monitoring system. Employee management is an aspect widely practiced in all workplaces. As day by day security breaches and transaction fraud increases, the necessity for secure identification and private verification technologies is turning into a good concern to the organization. Therefore, efficient management of attendance is to be attained. The methods which the system will include are Biometrics: Face Recognition and RFID smartcards (both combined into one system) for developing an advanced and secure AMS. This automated system will record the attendance of the employees in the organization environment and it will facilitate the admin to access the information of the employees.

Table 1: Table of Abbreviation

SR. NO.	Mnemonic	Full Form
1.	AMS	Attendance Monitoring System
2.	RFID	Radio Frequency Identification
3.	GUI	Graphical User Interface
4.	SQL	Structured Query Language
5.	DFD	Data Flow Diagram

SYSTEM OVERVIEW

The proposed system will have the integration of the two technologies that are:
1) Face recognition technique
2) RFID smart cards.
The employee will have client interface in which he/she can interact with the attendance system. He /she will provide input in 2 ways. The first input will be the Face of the employee which will be captured from the camera and the second input will be the RFID card of the employee which will contain the employee details.
Now, these 2 inputs are taken from the user and transferred to the computer for processing and validation. The system will match both the details i.e. image of the employee and Card details.

When the details of the card (name) matches with the face of the employee, then the user is valid user and his/her attendance will be marked, as shown in the Fig 1, else it will generate error and again ask for the input.

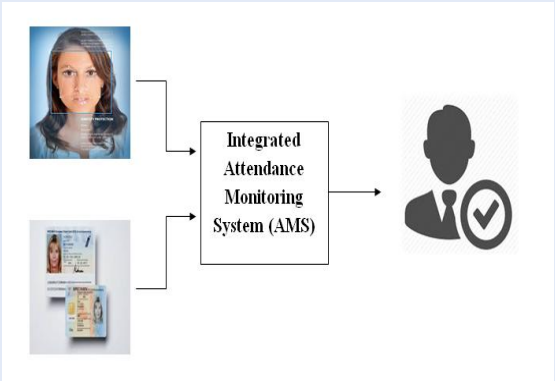


Figure1: AMS Module

METHODOLOGY

RFID CARD TAPPING

RFID stands for Radio Frequency identification, which is a technology that allows the user to communicate wirelessly with the RFID reader. It is possible to store and retrieve data with the help of the tag. A tag comprises of a microchip that is stored in RFID memory. This tag is affixed on the card of the employee which also serves as the ID card for the employee. Using RFID technology, the details of the employee, like Employee ID, Name, Contact No, Department etc., is stored on the tag. When the employee taps the card on the RFID reader, the details on the card is transferred to the system.

In cases of exceptions that occur due to some faulty or temporary circumstances like if the face is not detected, then an error message will pop up on the security systems' user interface with an alarm which will alert the security along with the details of the RFID card being tapped. The security can quickly access the foyer area through the installed CCTV camera and check by themselves whether the person is same as that mentioned in the RFID card details. If matched, the security can manually mark the employee's attendance through "Mark Attendance". If not, then the security can take any necessary action as shown in the Fig 2.

The RFID memory is rewritable which means that the details of the employee can be modified electronically multiple times as required. The RFID card used in this project operates at a frequency of 125 KHz and has a range up to 10 centimeters.

Figure 2: Security User Interface

FACE DETECTION AND RECOGNITION

The face of the employee will be captured through the camera fixed in the system. Face detection and recognition will be done using Viola Jones method which is proposed by Paul Viola and Michael Jones. For the face detection, Haar Cascade Classifiers are used to check the region of the face in the capturing window. The characteristic features of the face which the system detects are called as the Eigen face. The extraction of eigen face from the entire image is done by the means of Principle Component Analysis (PCA).

INTEGRATION

This Integration module is the combination of RFID card technology and Face Recognition. First the Employee will tap his/her RFID enabled ID card on the machine (reader), the system will extract the employee details from the card. At the same time, the system camera will detect the employees face and the system will recognize the employee with his name. The system will then check whether the recognized face matches the card details (Employee Name). If it matches, the system marks the attendance of the employee and signals the employee by Green LED light as feedback. If both the details fail to match, then the Security is prompted on their User Interface.

SYSTEM IMPLEMENTATION

The proposed system has been implemented with the help of three basic steps:

A. Detect and Extract the face from the given input i.e. Web Cam and store it in trainee set.

At first, grabber() is called to open the camera for image capture. Next the frontal face is extracted from the video frame by calling the function ExtractFace(). TheExtractFace() function uses the EmguCvHaarCascademethod to load the haarcascade_frontalface_default.xml as the classifier. The classifier can easily “Resize” the image of the different sizes, which is much efficient than changing the size of the image. When the employee face is detected the image is clipped into a 100x100 pixels grey scale image.

B. Calculate the Eigen value and Eigen vector of the image.

Principal Component Analysis (PCA) is used to find the Eigen value and Eigen vector. To calculate these values getEigenDistances() method is used. This method returns the eigen values to the function. For PCA, the Trainee dataset should be “centred”, that means we have to provide the image which should be cantered aligned. Now we find the average image of the employee using cvCalcEigenObjects() method. The cvEigenProjection() is used to reconstruct and project the Eigen values and Eigen vector of the image.

C. Recognize the face from the stored images in the Trainee set database.

Face recognize() function is used to recognize the face.GetEigenDistances() compares the Eigen value and Eigen vector from the every image in the database. After all the values are compared with the image using EigenProjection() method, we need to find the most similar image from the trainee data set to recognize the face. Once the most similar image is found it returns the value to the recognize() function so that the we get the name of that person. If the value does not matches with the any trainee set data, the error message will be shown that face could not be recognized.

Figure 3: Admin User Interface

SYSTEM FUNCTIONALITY

A. Get overall attendance

By using integrated attendance monitoring system we can easily get the overall attendance of the employee. The attendance record can be view weekly, monthly or according to our requirement. The attendance can also be viewed Department wise. All the information is generated in the form of Excel file generated by the system.

B. Employee details

System admin can easily view the employee's details as shown in Fig 3. These details can be Name, Contact Details, monthly attendance, reporting time, leaving time, total numbers of leaves, etc. Admin can also add or update the details of the employee. Search button facilitates searching Employee ID, Department ID.

PERFORMANCE

The overall timing required to mark the attendance of employee on both system separately requires around 20-30 sec approximately. To overcome this problem we are integrating both the system in a single place, so there is no need to mark the attendance separately at different places.
The AMS will mark the Attendance of the Employee within 3-5 seconds. This will reduce the time of marking the attendance significantly. The system proves to be more secure, as it uses both RFID technology and Face detection.

Figure 4: Face Recognition using EmguCV.

A. Security:

The attendance system must be fully accessible to only authentic user like Admin and Security. It should generate the error message when the input is not matched with the stored database records. This will avoid the proxy attendance.

B. Reliability:

The system should be highly reliable and it should generate all the updated information in correct order, so that we can rely on the system only.

C. Availability:

Any information about the employee should be quickly available. The previously visited employee's data must not be cleared; it should be stored in the database.

D. Maintainability:

The AMS System should be maintainable in such a way that if any new requirement occurs then it should be easily incorporated in an individual module. The system should be able to adapt the future changes that we are going to make.

CONCLUSION

The main drawback of using only RFID card was "Buddy-Punching" due to which proxy attendance is marked. So we designed an Automated Integrated System which will overcome all the drawbacks. Thus the implemented system will significantly improve the effectiveness in marking the attendance. This proposed and implemented automated system will be accurate and reliable to monitor the attendance of the employees.

FUTURE WORK

A. Visitor pass

When any outsider wants to visit the company or any employee in the workplace, his/her presence will be generated automatically by the means of a Visitor Pass. It will contain the details like Name, Contact Details, Reference of the person whom the visitor wants to meet and image of the visitor which will be the face captured by the AMS camera. This pass will be generated by the Security.

B. Tracking location

The system admin should know the exact location of the employee where he/she is working. This will ensure that the employee is present in his/her department only, not in other department. For this location of the employee within the work place can be tracked by the means of RFID Card. So admin can track the location of employee in the organization.

REFERENCES

[1] Yugandhara M. Bhage, Surabhi S. Deshmukh, " Automated Attendance Monitoring using face recognition", International journal for research in emerging science and technology ,Vol. 2,March 2015

[2] Sumita Nainan, Romin Parekh, Tanvi Shah, “RFID Technology Based Attendance Management System”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013

[3] Nirmalaya Kaur, Mrinal Kanti Debbarma, Ashim Saha, Dwijen Rudra Pal, "Study of implementing automated attendance system using face recognition technique", International journal of Computer and Communication Engineering Vol. 1,No.2(2012)

[4] Aniket Shah, Amruta Tuptewar, Pradnya Yeole, Prof. L. J. Sankpal, "Automated attendance monitoring and personal Intelligence system", International journal of advanced research in computer and communication Engineering, Vol.3, Issue 11(2014)

[5] Stan Z. Li and Anil Jain, Handbook of Face Recognition, Aug 31, 2011

[6] Asit Kumar Datta and MadhuraDatta, Face Detection and Recognition: Theory and Practice, Nov 20, 2015.

[6] Naveed Khan Balcoh, M. Haroon Yousaf, Waqar Ahmad and M. Iram Baig, "Algorithm for Efficient Attendance Management: Face Recognition based approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012

[8] Mohamed Daoudi and Anuj Srivastava, 3D Face Modeling, Analysis and Recognition, Aug 19, 2013.

About the Authors:

Mr. Prashant Prajapati, Department of Computer Engineering, Universal College of Engineering, Kaman, Vasai, India. prashant25@live.com

Sejal Patel, Department of Computer Engineering, Universal College of Engineering, Kaman, Vasai, India. sejukush@live.com

Prathamesh Sadekar, Department of Computer Engineering, Universal College of Engineering, Kaman, Vasai, India. sadekarprathamesh9@gmail.com

THE DEEP WEB: LET'S DIVE

WHAT IS DEEP WEB?

The deep web is actually a vast amount of information, which is not indexed and served up by traditional search engines like Google, Yahoo or Bing. It includes all kinds of places from academic database to private websites & corporate portals. These all resources are collectively known as "The Deep Web" or "invisible Internet".

Only 1% of content is accessible by the traditional search engines. This content is stored in file format. Hence, Google or Yahoo like search engines can't deal with or can be accessed using some dynamic database queries.

So, the deep web is not a place it simply counts unindexed content. The content may be like banking data, administrator code for corporation & universities.

HOW BIG IS DEEP WEB?

Some studies depicts that the size of the deep web is 450 to 500 times larger, deeper than the surface web. The surface web is the part of internet which is easily accessible through the search engines likeGoogle, Yahoo, etc. Let's assume that the World Wide Web as a iceberg. The following fig.(A) describes the World Wide Web as iceberg. The iceberg has two parts one is surface web & another the deep web. The surface web is the content on the internet which can be easily accessible by anyone on the internet. The surface web is considered as the top of the iceberg. The search engines like Google, Bing, Yahoo, etc. can crawl to these surface web's web pages. At the bottom part of iceberg the deep web is present. Study done by university of California, Berkley in 2001 concluded that the deep web is about 7.5 petabyte (7500GB) in size. After three years in 2003 another survey was conducted on deep web ,the report stated that the size was increased to 91850 petabyte. Still up to current date the size of deep web is increasing.

Figure (A):Size of deep web & surface web

After looking at the size of the deep web now, let's dive more deep to these ocean.

HOW TO DIVE INTO THIS DARK INTERNET OR DEEP WEB?

The deep web has its secrets, hidden in so much deep that the normal search methods or search engine crawlers like Google, Yahoo, etc. cant index to those web pages or content. So to dive into this ocean of information there are some tools, for example TOR (onion router) browser, I2P browser, Tails OS, Orbot (for android smartphone).

A) TOR (onion router): Onion router was funded by firstly developed by non-profit group called TOR project. Today it is just a anonymity browsing system & it's sponsored by U.S. Government.
B) I2P Browser: This browser works just as alternative for TOR. In this P2P software is employed.
C) Tails OS: The Tails OS is Linux distribution &TOR OS. It provides anonymity to user.
D) Orbot: Orbot is tool for Android smartphones. Which provides anonymity traffic from the web browser through the TOR network.

SOME INTERESTING FACTS ABOUT DEEP WEB:

Silk Road: SilkRoad was launched on February, 2011. Its hidden marketplace to buy drugs (Illegal), weapons, etc. over 13000 items are present on the silkroad for sell.
Bitcoin: A digital currency called Bitcoin, introduced in 2009. The value of Bitcoin costs about 250 USD (230 Euros). Which is used during the transaction on the sites like silkroad, hitmen, etc. It's an encrypted currency which offers anonymous transaction. The bitcoin service don't share identity of seller & buyer.
Journalists from countries like North Korea where internet censorship is very high. So, reporters & journalists use deep web to research & to look for the current trends in the outside world, as well as to exchange information between other reporters present outside the world.

The deep web provides anonymous email services to the journalists & reporters in countries like North Korea to communicate with the outside world.

About the Author:

Mr. Onkar Uttam Patil [CSI membership ID -01319338] is currently studying in third year of Engineering at Dr. J. J. Magdum college of Engineering and Technology, Jaysungpur.

TOP10 TOOLS FOR NATURAL LANGUAGE PROCESSING (NLP)-RESEARCH AND DEVELOPMENT

Compiled by:

Anand Nayyar and Vikram Puri

The main goal of Artificial Intelligence till date since its development is to develop various intelligent computational methods for understanding natural language. Since the inception of research of machine learning, numerous challenges have been faced regarding word translation and word identification. The Research has showed in recent times, that to understand natural language requires not only lexical and grammatical information but semantic, pragmatic and general world knowledge. However, the development of accurate natural language processing systems is till date difficult to design as it requires a great zeal of domain-specific knowledge engineering. The systems developed till date are also not very accurate and has limited environment to operate accurately.

WHAT IS NATURAL LANGUAGE PROCESSING (NLP)?

HISTORY

Talking of History of NLP, when in 195-s, Alan Turning published an article titled “Computing Machinery and Intelligence” which is now regarded as Turing Test as a criterion of intelligence. Some NLP systems like SHRDLU was developed in 1960s, ELIZA based smart Artificial Intelligence systems developed in 1964-66 by Joseph Weizenbaum. In 1970s many programmers wrote ‘conceptual ontologies’ such as MARGIE, SAM, PAM, TaleSpin, QUALM, Politics and Plot Times.

DEFINITION

Natural Language Processing (NLP) is a mixture of three fields: Computer Science, Artificial Intelligence and Computational Linguistics and was developed basically for providing a bridge between computers and human languages understanding. So, NLP is often referred to as “Human-Computer Interaction”. Human being speak natural languages and human understand natural language from environment where they use some language as medium to interact with other humans. Natural Language is being learnt from childhood. Till date, there is no Methodology available where these languages in all of their unprocessed forms can be understood by computers. Natural Language Processing is defined as collection of techniques and tactics developed and employed to make the computers understand natural languages. Natural Language Processing (NLP) comprise of various techniques used to extract grammatical structure and meaning from input to do a useful task as a result, NLP helps in building output based on rules of the target machine and task at hand.

The main objective of Natural Language Processing is to measure qualities of algorithm or system being developed to determine whether the developed algorithm by the researcher meets the need of users and how much accuracy it has in processing the natural language. The evaluation of algorithm allows for integration of language understanding and language generation. But till date, no proper research criteria and evaluation analysis methodology is being developed and proposed for testing the suitability of algorithm proposed to test its practical viability and applicability. The research field of Natural Language Processing is very vast and requires lots of more accurate research models and algorithms for testing the suitability and accuracy. NLP nowadays is being used in various areas like Machine Learning, Test Processing and Summarization, User Interfaces, Cross Language Information Retrieval (CLIR), Artificial Intelligence and Expert Systems and so on.

The objective of this article is to highlight various tools available till date for researchers and developers for doing research in NLP and testing their algorithms proposed and developed.

Tools Available to Natural Language Processing

In this section, various Top Tools available for Natural Language Processing are being highlighted:

1. Apache OpenNLP: Apache OpenNLP is a machine learning based toolkit for processing natural language text. Apache OpenNLP supports various NLP tasks like Tokenization, sentence segmentation, part-of-speech tagging, named entity extraction, chunking, parsing and coreference resolution. The Latest version available for download from www.opennlp.apache.org is 1.6.0. It is free and open source tool for NLP.
2. Stanford CoreNLP: StandfordCoreNLP provides a set of NLP tools and provides easy interface for doing research on NLP as the toolkit is highly flexible and extensible. Stanford CoreNLP includes various tools like part-of-speech (POS) trigger, the named entity recognizer (NER), the parser, the conference resolution system, sentiment analysis, bootstrapped pattern learning and the open information extraction tools. The main use of this toolkit is in domain-specific text understanding applications. Toolkit can be downloaded from http://stanfordnlp.github.io/CoreNLP/ and the latest version is 3.6.0.
3. ScalaNLP: ScalaNLP is regarded as suite of machine learning and natural language processing. ScalaNLP comprise of libraries: Breeze, Epic and Puck. The updated version is named as ScalaNLP Breeze with contains addon libraries for Linear Algebra, Numerics, Machine Learning and NLP in Scala. ScalaEpic is regarded as powerful, statistical parser for eight languages backed by a generic framework for building complex systems using structured prediction. Puck is fast GPU powered parser and can parse 400 sentences a second, over half million words per minute. The latest version of ScalaNLP is 2.9.2 and can be downloaded from http://www.scalanlp.org/

4. Snowball: Snowball is a string processing programming language which is designed for the objective for creating stemming algorithms to be used in information retrieval. Snowball comprise of a compiler whose basic task is to translate Snowball script into C or Java Programme. Data types which are being used by Snowball are string of characters, signed integers and Boolean truth values or simple strings, integers and Booleans. Snowball was created by Dr. Martin Porter as Snowball provides a 'suffix STRIPPER GRAmmar". Snowball can be downloaded from http://snowball.tartarus.org/download.php

5. MALLET: MALLET (Machine Learning for LanguagE Toolkit) is regarded as important package based on JAVA programming language for statistical natural language processing, document classification, clustering, topic modelling, information extraction and other machine learning applications to text. Mallet was developed by Andrew McCallum by University of Massachusetts Amherst. MALLET is open source and is available free of cost to download from http://mallet.cs.umass.edu/download.php and the latest version is 2.0.8. MALLET also includes various routines for transforming text documents into numerical forms in order to facilitate efficient processing and is done via system of pipes.

6. JGibbLDA: JGibbLDA is regarded as Java implementation of Latent Dirichlet Allocation (LDA) using Gibbs Sampling technique for parameter estimation and inference. The main goal of JGibbLDA is on inferring hidden/latest topic structures of unseen data upon the model estimated using GibbLDA++. The framework provides a easy to use API to get topic structures for an array of input strings. LDA was developed by David Blei and this model has been implemented in C, Java and Matlab. The areas where JGibbLDA can be applied are: Information Retrieval, Document Classification/Clustering, Object Recognition, Computer Vision, Collaborative Filtering and other image processing research areas. JGibbLDA can be downloaded from https://sourceforge.net/projects/jgibblda/ and the latest version is 1.0.

7. Apache Lucene&ApacheSolr:

Apache Lucene: Apache Lucene was developed by Doug Cutting and is completely developed in Java and is regarded as free and open source information retrieval software library. Lucene is now available in varied programming languages like Delphi, Perl, C#, Python, Riby and Php. Apache Lucene provides powerful and efficient search algorithms like Ranked searching, fielded searching, multiple-index searching with merged results, flexible faceting, pluggable ranking models. The Latest version of Apache Lucene available for download at : https://lucene.apache.org/ is 5.5.0.

Apache Lucene Includes the following Modules:

- Lucene Core: Provides java-based indexing and search technology like spell checking, hit highlighting and advanced analysis/tokenization capabilities.
- Solr: High performance search server built on lucene core with XML/HTTP and JSPN/Python/Ruby APIs and provides various facilities like hit highlighting, faceted search, replication, caching and web admin interface. The Latest version available for Solr is 5.5.0
- Pylucene: It is regarded as Python port of the Core Project of Apache Lucene.

8. Stanford Topic Modelling Toolbox: The Stanford Topic Modelling Toolbox (TMT) provides modelling tools to social scientists and other researchers a good platform to perform analysis on datasets which have a high textual based data. TMT tool imports and manipulates text from various cells in Excel and other spreadsheets based softwares. TMT Tool also generates Rich- Excel compatible outputs for tracking word usage across topics, time and other groupings of data. Stanford Topic Modelling Toolbox was developed by Daniel Ramage and Evan Rosen from Stanford University and the TMT toolbox can be downloaded from http://nlp.stanford.edu/software/tmt/tmt-0.4/ and the latest version is 0.4.

9. Natural Language Processing ToolKit with Python: Natural Language Processing Toolkit with Python (NLTK) comprise of suite of open source program modules, tutorials and problem sets for ready to use computational linguistics courseware. NLTP is purely written in Python and is available

as open source and free to downloaded. NLTP was designed taking into consideration the 4 primary goals: Simplicity, Consistency, Extensibility and Modularity. NLTP consists of large collection of minimally interdependent modules organized into a shallow hierarchy. Core Modules defines basic data types which are used throughout the toolkit. The remaining modules are task modules, devoted to individual natural language processing task. NLTP Library includes: Lexical analysis; n-gram and collocations; Part-of-Speech tagger; Tree model and Text chunker for capturing; Named-entity recognition. NLTP can be downloaded from http://www.nltk.org/ and the latest version is NLTK 3.0.

10. GATE and Apache UIMA:

GATE: GATE(General Architecture for Text Engineering): It provides strong platform to solve almost any text processing problem and is armed with defined and repeatable process for creating robust and maintainable text processing workflows and is currently used in varied applications like Recruitment, web mining, information extraction, decision support and many more. GATE has a suite of Java tools and includes an information extraction system called ANNIE (A Nearly New Information Extraction Systems) which consists of tokenizer, gazetteer, sentence splitter, part of speech dragger and coreference tagger. GATE takes input from various files like txt, html, XML, PostgreSQL, Oracle RDBMS etc. GATE can be downloaded from https://gate.ac.uk/download/ and the latest version is GATE Developer 8.1.

Apache UIMA: UIMA (Unstructured Information Management Architecture) is a component architecture and software framework implementation for data analysis of unstructured content like text, video and audio data. The aim of Apache UIMA is to transform unstructured information to structured information by orchestrating analysis engines to detect entities or relations thus providing a huge bridge between unstructured and structured data. UIMA is a component software architecture used for development, discovery, composition and deployment of multi-modal analytics for the analysis of unstructured information and its integration with search technologies developed by IBM. Apache UIMA can be downloaded from https://uima.apache.org/downloads.cgi and the latest version is 2.0.1.

CONCLUSION

Natural Language Processing is a strong area of research which mixes various allied field. Till date, no as such accurate model is being developed for processing natural language. So, lots of research is being required in Natural Language Processing area for development of text searching, document analysis, processing of text etc. like topics and development of new models, techniques and algorithms for the same. In this article, top 10 NLP tools are being listed which will enable the researchers as eye-opening platform to make use of these tools in diverse areas of their respective research and propose and test new algorithms and models being developed for NLP.

REFERENCES

1. Cambria, E., & White, B. (2014). Jumping NLP curves: a review of natural language processing research [review article]. Computational Intelligence Magazine, IEEE, 9(2), 48-57.
2. Chowdhury, G. G. (2003). Natural language processing. Annual review of information science and technology, 37(1), 51-89.
3. Jones, K. S. (1994). Natural language processing: a historical review. InCurrent issues in computational linguistics: in honour of Don Walker (pp. 3-16). Springer Netherlands.
4. Bird, S., Klein, E., &Loper, E. (2009). Natural language processing with Python. " O'Reilly Media, Inc.".

5. Loper, E., & Bird, S. (2002, July). NLTK: The natural language toolkit. In Proceedings of the ACL-02 Workshop on Effective tools and methodologies for teaching natural language processing and computational linguistics-Volume 1 (pp. 63-70). Association for Computational Linguistics.
6. https://opennlp.apache.org/ (Accessed on March 20, 2016)
7. http://stanfordnlp.github.io/CoreNLP/ (Accessed on March 20, 2016)
8. http://www.scalanlp.org/ (Accessed on March 20, 2016))
9. http://snowball.tartarus.org/ (Accessed on March 20, 2016)
10. http://mallet.cs.umass.edu/ (Accessed on March 20, 2016)
11. http://jgibblda.sourceforge.net/ (Accessed on March 20, 2016)
12. https://lucene.apache.org/ (Accessed on March 20, 2016)
13. http://nlp.stanford.edu/software/tmt/tmt-0.4/ (Accessed on March 20, 2016)
14. http://www.nltk.org/ (Accessed on March 20, 2016)
15. https://gate.ac.uk/ (Accessed on March 20, 2016)
16. https://uima.apache.org/ (Accessed on March 20, 2016)
17. Bird, S. (2006, July). NLTK: the natural language toolkit. In Proceedings of the COLING/ACL on Interactive presentation sessions (pp. 69-72). Association for Computational Linguistics.

About the Authors:

Er. Anand Nayyar[CSI-I1502825], working as Assistant Professor in Department of Computer Applications & IT at KCL Institute of Management and Technology, Jalandhar, Punjab. He is having 9 Years of Teaching Experience. He has chaired many national and international conferences and has published more than 250 Research Papers. His area of interests includes Wireless Sensor Networks, MANETS, Cloud Computing, Network Security, Swarm Intelligence and Embedded Systems. He is Life Member of CSI-India and Senior Member (ACM).

Er. Vikram Puri [CSI-1161622] is currently working as Corporate Trainer and Embedded Systems Engineer in Enjoin Technologies, Jalandhar. His area of interests includes Embedded Systems, Real Time Systems, Robotics, Microcontrollers and Programming in C/C++. He is member of ACM, theIRED, CSI-India.

UNDERWATER SENSOR NETWORK(UWSN)

Compiled by:

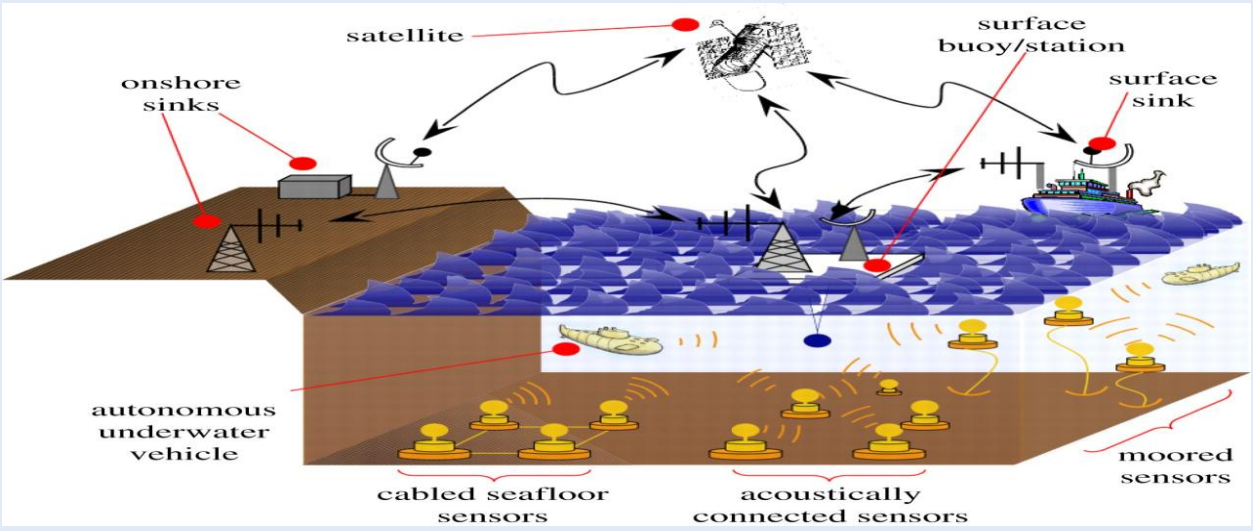
Harisubramanian.S , T.Kalaichelvi and S.Venkata Lakshmi

INTRODUCTION

Almost 75 percent of earth is covered with rivers, seas, canals and oceans. There are plenty of precious resources which lie under water that are to be explored. Under water sensor network (UWSN) technology leads to the possibilities to do underwater explorations. UWSN is a fusion of wireless technology with small micromechanical sensor technology having intelligent computing, smart sensing, and communication capabilities.

USWN TECHNOLOGY

Underwater wireless sensing systems contains stand-alone applications and control of autonomous underwater vehicles. For example: wave sensors, seismometers and cameras. Communication access points support cables which is a cellular base stations connected to telephone network, it allows users to communicate from one place to another where cables don't reach.



APPLICATIONS

- Long-term aquatic monitoring, water quality monitoring, habitat monitoring, and monitoring underwater explorations.
- Oceanography, , oil/gas field monitoring, seismic predictions, pollution detection

- Sea web is a large deployable network for military applications

- prediction of natural disturbances, instrument monitoring, pollution control, survey missions,climate recording.

Example: Remotely operated vehicles (ROVs). These type of vehicles weigh of about 10 metric tonnes and more are connected to mother ship which can extend several kilometers and deliver a very high power and high speed signals

CHARACTERISTICS

- Narrow available bandwidth
- Radio is unsuitable for underwater sensor networks
- Must use acoustic channels
- High attenuation
- Very slow acoustic signal propagation : $1.5x10^3$ m / sec vs. $3x10^8$ m / sec

DISADVANTAGES

Real time monitoring not possible in this technology. The data recorded cannot be accessed until instruments are recovered .

Interaction is not possible between onshore control systems and monitoring instruments

FUTURE WORK

- Develop a complete package for all layers
- Validate acoustic model with measurements

About the Authors:

Harisubramanian. S is final year B.E Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Dr. T. Kalaichelvi is Professor Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA.

Mrs. S. Venkata Lakshmi is Assistant Professor ,Computer Science and Engineering at Panimalar Institute of Technology in Chennai, Tamil Nadu, INDIA

VIRTUAL REALITY AND ITS APPLICATIONS

Compiled By:

Rasmiya Najeem and Nileena Thomas

ABSTRACT

Virtual reality is complex user interfaces which includes simulations in real time, and are achieved through sensory channels like visual, auditory etc. It enables you to actively participate in a 3-dimensional computer simulated world. This paper defines what virtual reality is and about its application in different areas and the different technologies and devices used in it for providing real-time experience.

INTRODUCTION

Imagine that there is an authenticity in virtual world, you can do everything in it, and you can live in it and can spend your whole life there itself. From real and fact's point of view nothing is real. Basically the concept of virtual reality comes from dream. When you see a dream, everything appears real to your brain, sometimes you are trying to save yourself and are moving your hands and legs and your body got sweat and you are even talking but that dream world only exists in your brain. Nothing is real in dream. But the fact is that dream tricks your brain and the brain believes it because of an illusion given by the dream that everything is real. As the brain controls the whole body it gives orders to the different organs which are concerned

For example, Let us suppose that someone is seeing a dream that an animal is in front of him and it will kill him. Now the brain thinks that everything is real so the brain commands the leg to run fast. Similarly the brain commands the hands to move also it commands the skin to sweat and commands the heart to beat fast because of fear. Now when we think about the real and fact's position that there is no animal in real and everything is virtual but brain is thinks that everything is real. So it is from here where the concept of virtual reality comes. The example given above shows us that we can trick the brain by making it think that the virtual world is real.

The very simplest form of virtual reality is a 3-D image that can be studied interactively at a computer, usually by manipulating keys or the mouse so that the image moves in some direction or zooms in or out. More advanced efforts involve approaches as wrap-around display screens, actual rooms improved with wearable computers, and haptics devices which let you feel the images displayed.

Virtual reality can be divided into two:

1. The recreation of a real environment for education and training.

2. The development of an imaginary environment for a game or interactive story.

Virtual Reality can be applied in many areas:

1) It can be used in study of medicine to allow students to know the human body structure.

2) It can be used in research laboratories so that scientists can easily research on different topics.

3) It can be used in entertainment like in games, movies, etc. to make the experience more real.

4) It can be used in driving schools, as it gives a real look of roads and traffic.

5) It can be used for training the military force to get familiar with the battleground.

TECHNOLOGY

Technology is very complex in terms of its working but it is very simple in terms of usage its materials used that contains.

1. Goggles

2. Suit for different parts of body

In goggles there are two TV like screens instead of glasses. These screens are made from best technology to give the output of the image close to reality. The suits basically for the body, we fix suit with body, then we switch on the TV screens and the person wearing the goggles can see world in it. This world seems so real that the brain goes into it and thinks that it is real.

Now if we get the same world to appear on the screens in the apparatus and the graphics used in that imaginary world are as real as the scenes of our real world. Then the brain will get the illusion that the world is real and it will start working according to it. Now let me give you an example which will explain you the working of goggles and suits. Suppose in virtual reality we see a chair. Now the brain thinks that it is a chair now if we touch the chair we'll know that there is no chair but the person wearing the goggles and having suit fixed on his body will feel the chair. You will be thinking how.

The person will imagine or feel it because of pads/suit. The pads on the person's fingers will give the illusion of sturdiness of wood and also its feel. The fingers gives the signal of the feeling it gets and then the signal goes to brain and brain interprets it and gives the body a feeling that it is a chair. Now actually there is no chair but goggles and suits mislead our brain by giving it illusion that it is a chair.

This is how virtual reality works.

Input Devices and other Sensual Technologies:

Different input devices like data gloves, joysticks, and hand-held wands allow the user to move through a virtual environment and to communicate with virtual objects. Directional sound, force feedback devices, voice recognition and other technologies are being introduced to improve the indulgive experience and to make a more sense inducing interfaces.

HEAD-MOUNTED DISPLAY (HMD)

The head-mounted display (HMD) was the first device giving its wearer with an indulging experience. It took more than 20 years before VPL Research came up with a commercially available HMD, the "Eye Phone" system in 1989.

A typical HMD has two small output screens for display and an optical system that connects the images from the screens to the eyes, thereby, giving an audible view of a simulated world. A tracker continuously measures the motion, the position and space of the user's head and allows the picture generating computer to adjust the scene representation to the present view. As a result, the person can look around and walk through the virtual environment. To overcome the often discomfort of a head-mounted display, other concepts (e.g., BOOM and CAVE) for indulging viewing of virtual environments were developed.

BOOM

The BOOM (Binocular Omni-Orientation Monitor is a head-coupled audio display device. Screens and optical system are placed in a box which is connected to a multi-link arm. The user looks into the box through two holes, sees the imaginary world, and can move the box to any position within the operational space of the device. Head tracking is done by sensors in the connectors of the arm that holds the box.

CAVE

The CAVE (Cave Automatic Virtual Environment) was made at the University of Illinois at Chicago and gives the illusion of immersion by giving out audio images on the walls and floor of a room-sized cube. People wearing lightweight stereo glasses can enter and move freely inside the CAVE. A tracking system tracks the head movement throughout adjusts the projection to the current position of the viewer.

IMMERSIVE AND NON-IMMERSIVE TECHNOLOGY

NON-IMMERSIVE TECHNOLOGY

A non-immersive reality is one in which only some of the senses are included. This leaves the person having some awareness of the reality outside the VR, as direct sensory awareness.

For example, at the same time as your eyes and ears may be in the simulation, your fingers is still feeling the desk in front of it.

IMMERSIVE TECHNOLOGY

In a virtual reality environment, a person experiences a feeling of being inside and becoming a part of that world (immersion). He is also able to interact with his environment in different meaningful ways. The blend of sense of immersion and interactivity is known as telepresence. So this virtual reality experience will make u unaware of the real world surrounding and will make you focus on your existence in the virtual surrounding.

4. APPLICATIONS

Useful applications of this concept include training in a several areas like military, education, medical, equipment operation, design evaluation i.e. virtual prototyping, architectural walk-through,

human factors and, study and treatment of phobias (e.g., fear of water), entertainment, and much more.

It is assumed that virtual reality will reconstruct the interface between the information technology and the people by providing new ways for the communication the visualization of processes, and the creative expression of ideas.

MEDICAL

Virtual reality technology in medical field is rapidly growing, which will change the face of health care in the future. In the past decade the focus of this technology on medical field had been developing quickly and the technology has changed to a commercial from a research.

Doctors getting trained in Virtual Hospital

The most promising application fields for virtual reality technologies are education and training fields. It will be very useful for medical students to learn real world practical problem in virtual reality world. For example Medical students can do surgery on a patient who will be dying due to some disease in a VR world.

Image Guided Surgery

Image guided surgery is the common application area where virtual objects like the data from the preoperative data and the anatomical items separated from them and real objects like the patient and the surgical tools must be merged into a single scene, calling for better reality techniques. The major technical problem to be solved is to make the preoperative data sync with the actual patient analysis and the tracking of real objects such as the surgical instruments.

Preoperative planning

In many areas the use of computer models to plan surgical involvement preoperatively is part of daily clinical practice. In some areas, treatment is not possible without preoperative planning (like conformal radiotherapy and stereotactic neurosurgery).

AERONAUTICAL TRAINING PROGRAMS

Virtual Reality has a very important role in Aeronautics which is very helpful for Air force, Navy, Army etc.

Flight stimulators

We can train pilots with the help of flight simulators (based on virtual reality).

Virtual Reality Parachute Training

Due this technology the risk and fear of life can be totally avoided.

Aircraft Designing Programs

With the help of such technology, they can easily check every corner and the movement of air on the body of the aircraft.

WORLD TOUR

We can explore the world with the help of VR technology.

Imagine you are sitting in your home at Kochi and if u want to visit some foreign place you can take a visit sitting in your home itself and if you didn't like that place you can go to somewhere else like London within a few seconds and can enjoy the summer or winter with a click of a button.

VIRTUAL TEACHING PROGRAMS:

A student can graduate and thus get education from the professors and can enjoy the campus and environment of different universities. A teacher can develop their teaching skills by taking class in a virtual reality classroom at any university which provides the same atmosphere like real classrooms.

CONCLUSION

By 2030 both the simulation and interface technologies are likely advance to a level sufficient for a perfect Matrix-like imitation identical to reality, but the virtual avatar will still be controlled by the human brain. While the Matrix scenario of immobile humans immersed in a medium and in a VR permanently is possible, and it is expected that most people would spend more of their time in virtual physical reality than in the real world.

Technological development in virtual reality is expected to be:

•2010-2015: video-realistic graphics based on general-purpose constant rendering systems.

•2015-2020: integrated stable worlds,

Global physics with unlimited world complexity, sufficiently good non-human and province specific human AI.

•2015-2025: programmatic sound, realistic simulations of all senses by means of brain-computer interface.

•2030+: human-level artificial intelligence.

•2045+: life in virtual reality.

AKNOWLEDGEMENT

We, Nileena Thomas, Rasmiya Najeem, and thank almighty god, our parents, and our institution-Amrita School of Arts and Sciences for giving us this opportunity for presenting this paper. We also thank Computer Society of India (CSI) for organizing such an event.

REFERENCES

1. http://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.html
2. http://www.vrs.org.uk/virtual-reality/what-is-virtual-reality.html*https://en.wikipedia.org/wiki/Head-coupled_perspective

3. http://science.howstuffworks.com/virtual-military1.html
4. http://www.w2vr.com/archives/Fisher/07a_Boom.html

About the Authors:


RASMIYA NAJEEM
CSI:01333135


NILEENA THOMAS
CSI:01333131

Amrita VishwaVidyapeetham
Amrita School of Arts and Sciences, Kochi

VIRTUAL REALITY

compiled by:

Kartik Nagpal

INTRODUCTION

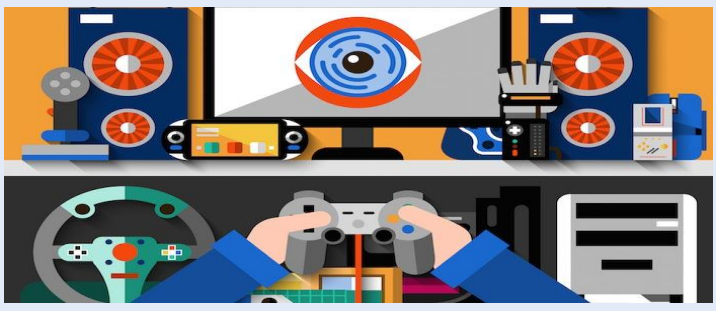
Our world is changing with the speed more than ever before and this has gained significantly after the introduction of computers. Since then, the human imagination and thinking are reaching the new heights. Boring work is undertaken by the computers and most people are working towards making something new. Now, humans are not satisfied with the available technologies and they want more. This is proved by the fact that last few years have changed our world more than previous decades. Some of the technologies which are developed in last few years are 3-D technology, Virtual Reality, Artificial Intelligence and Human Interactive Environments.

Virtual Reality is a technology which is changing our world and yet to reach its true capabilities. It has been discovered a few decades back but was not useful at that time due to lack of hardware. Today, few companies are dedicated to making virtual reality devices and testing the capabilities of this technology. It was firstly developed in the 1960s as a head mounted display which was too heavy to be worn. It was primitive both in terms of user interface and realism.

WHAT IS VIRTUAL REALITY?

The definition of virtual reality comes from both the terms ‘virtual’ and ‘reality’. The definition of ‘virtual’ is near and reality is what we experience as humans. So it basically means ‘near-reality’. It is a technical term used to define a three-dimensional and computer generated environment which can be interacted, explored and immersed with by a human.

Virtual Reality is a technology that allows a user to interact with a simulated environment which can be real or imagined. It simulates a user’s physical presence and environment to allow for user interaction. Some virtual realities artificially create a sensory experience, which can even include other human senses like touch, hearing, and smell. Most current virtual realities are displayed either on a computer screen or with a virtual reality headset (also called head mounted displays) and some simulations include sensory information and focus on real sound to provide much real experience. The virtually simulated experience can be similar to the real world in order to create a lifelike experience or create a totally imagined environment and completely differ from reality.



APPLICATIONS OF VIRTUAL REALITY

In past, Virtual Reality has been used by pilot training and military training because VR devices were very costly and could not be afforded by users. But now, these are better than ever before and cheaper. This technology has got so much potential that it could be used for various purposes.

Virtual Reality seems like a lot of effort and it is! What makes its development worthwhile? The potential entertainment value is clear. Entertainment is the biggest business and Immersive films and video games are good examples. The entertainment industry is multi-billion dollar one and consumers are always keen on novelty. Virtual Reality has many other applications which are rather more serious which are:

- Architecture
- Medicine
- Sports
- Entertainment (Films and Video Games)
- The Arts
- Heritage and archaeology
- Retail
- Therapy
- Training

Big steps are being taken in the realm of education, although much needs to be done. Some are creating education content for using in the virtual environment. The classes can be held online in a Virtual reality classroom where everyone is present from different parts of the world through telepresence. Driving training, Space Suit training or any other kind of training can be done in a virtual environment without taking any risk of any real damage. Virtual Reality has been introduced at some theme parks to provide more immersive and real experience. Some big retail stores have introduced virtual reality to provide the proper knowledge of the product which the buyer needs. Big production houses are using Virtual Reality campaigns to promote their movies and providing a much closer look to the audience.

Whenever it is too impractical, dangerous or expensive to do something, virtual reality is the answer. From checking building designs, trainee fighter pilots to medical applications trainee surgeons, virtual reality allows you to take risks in a virtual environment and providing the real experience providing a chance to improve from your mistakes.

VIRTUAL REALITY IN FICTION

Long before when virtual reality was not in usable form, many books and movies have shown something similar to what virtual reality is now. Many movies have imagined characters trapped in virtual reality. Some people has shown virtual reality a way of getting out of the misery of reality. The basic idea of virtual reality came from the movies and these movies also explored the potential of virtual reality.

Movies like Star Wars and Star Trek showed the pilots training in virtual environments by putting headsets. Video game developers have truly explored the potential of virtual reality and trying to make the fully functional imagined virtual environment which adapts according to the user.

The 1993 film Arcade was centered around a new virtual reality game which can actively traps who play it inside its world. The movie also got a name from that game.

The 1999 film The Thirteenth Floor which is an adaption of Daniel F. Galouye's novel Simulcron-3 and tells about two virtual simulations, one in another.

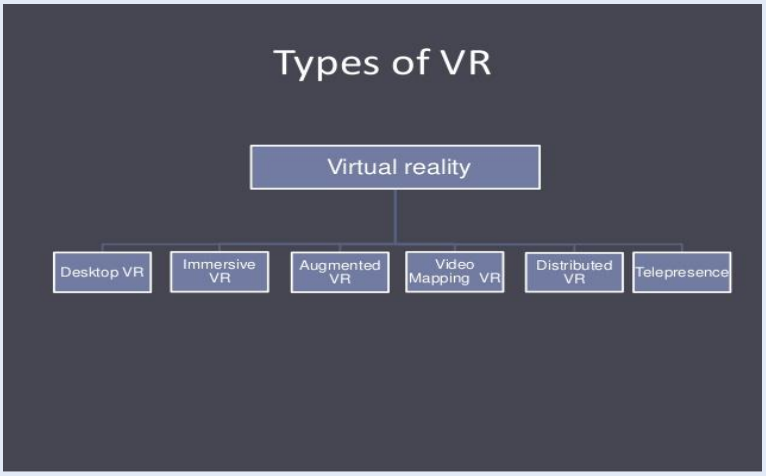
Matrix and later sequels released after 1999 explored the possibility that out the world exists in a virtual reality and all people, in reality, are sleeping in deep sleep and this virtual reality is created by artificially intelligent machines.

Video games, nowadays, are immersive and adaptive according to the user and user can explore the imagined world and can interact with other characters who are controlled by other humans or computer generated.

TYPES OF VIRTUAL REALITY

There are many types of Virtual Reality, which are as follows:

- Desktop Virtual Reality
- Immersive Virtual Reality
- Augmented Virtual Reality
- Telepresence
- Distributed Virtual Reality
- Distributed Virtual Reality



Immersive VR provides an immediate, first-person experience. Immersive systems involve computer interface devices such as head-mounted display(HMD), fiber-optic wired gloves, position tracking devices, and 3-D surround sound audio systems.

Augmented Reality is the variation of immersive Virtual Reality. In this, there is an overlap of a see-through layer of computer graphics over the real world to highlight something. This type of reality is used in a device HoloLens developed by Microsoft.

Telepresence is the feeling of being in a location other than were you actually are. It means controlling a robot or any other device from a distance. The device which can perform actions on the commands given by the user.

Virtual Reality applications can be divided into two types:

1. The simulations of real environment such as the design of a building, interior of an aircraft with the purpose of training and education

2. The development of an imagined environment which is in video games and movies.

VIRTUAL REALITY DEVICES

Most people are guessing that the next big thing in the world of computers is Virtual Reality and it's already here. 2016 is the year when devices like PlayStation VR, Oculus Rift, and HTC Vive take virtual reality mainstream. With these devices in the hands of gamers and other users, the revolution in already under way. Many companies have started to work on VR devices seriously and have presented some products to the users like HTC Vive, HoloLens, PlayStation VR and Oculus Rift.

HTC Vive is the Steam VR headset made in collaboration with Valve and HTC. The HTC Vive plugs into PCs and works with Valve's gaming ecosystem. It works with 70 sensors to offer 360-degree head-tracking as well as a 90Hz refresh rate.

Oculus Rift is the virtual reality headset developed by a company Oculus, which was one of the first to enter the race. This company is now acquired by Facebook for $2 billion. This device plugs into your computer's DVI and USB ports and tracks your head movements and changes according to it to provide 3D imagery on its stereo screens.

The PlayStation VR is the headset which is yet to be launched. A prototype of this device was shown last year. This device will have a 5.7-inch OLED screen which enables low persistence, which should mean less motion blur. When launched, this device could be used with PlayStation devices.

Microsoft HoloLens is not a copycat of other big VR headsets, it blends virtual and augmented reality to make it one of the most ambitious launch. It merges the real-world elements with virtual 'holographic' images, which means you could see a virtual aircraft in your garden or walk around the surface of the moon in your living room.

Several other devices have been launched and most of these devices are actually in beta stage and needs improvement. Content for these VR devices is also worked upon and it will start coming out as soon as these devices are built completely.

PROBLEMS AND CHALLENGES

There are several health and safety considerations of virtual reality. For example, a number of unwanted symptoms which are caused by the prolonged use of virtual reality devices and these problems have slowed down the proliferation of this technology. In addition to this, there are some social, philosophical and conceptual considerations with virtual reality. The overuse of virtual reality can make a person socially cut-out and it can also become difficult to differentiate between the real world and the virtual world.

Some books and movies have also touched the negative part of this technology. In movie Matrix, all people are in virtual reality and they don't know if they are in the real world or virtual world. Machines have overtaken the cities and people are still in the virtual world.

This technology faces a number of challenges, most of which includes motion sickness and some technical matters. Users might become disoriented in a purely virtual environment and this can cause balance issues or maybe computer latency might affect the simulation. The virtual world should be close to reality and fast enough to adapt according to the user. Less than satisfactory end-user experience also results in bad reviews. The complicated nature of virtual reality devices like

specialized gloves, boots, and head-mounted displays is also keeping the people away from these devices.

The visual aspect of VR is close to being solved, but there are other areas of VR which needs solutions, such as 3D, audio, haptics, body tracking, and input. There is a rising concern that with the advent of virtual reality, some users may experience virtual reality addiction.

CONCLUSION

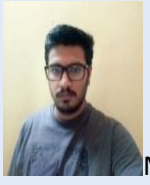
The concept of Virtual Reality is old, but its usage is possible only now. The hardware is now fully ready to accommodate the virtual reality simulated environments. Moreover, companies are now willing to invest in new technologies and taking risks. The possibilities are endless in virtual reality, all it needs is the idea.

Video game developers are working to make games fully functional virtual reality. Some developers are almost ready to launch games. One such game is 'No Man's Sky'. This game is set in an imagined reality and it is an exploration game in which user can travel to thousands of planets. The game will also come for virtual reality devices to provide the real experience.

Although there are some problems with this technology, but the work is done to remove any kind of side-effects of this technology. Every good thing comes with its fair share of problems but it is onto us to remove them and use the technology efficiently. Devices are being made and improved to be 100% ready and most probably, there will be full-fledged launched by the end of this year. Smartphones expand with so much speed which no one expected. In technology, computers bring the revolution. Then smartphones were the next big thing to bring the change. Maybe, Virtual Reality is the next big thing of the future.

REFERENCES

1. www.wikipedia.com
2. http://www.wareable.com/headgear/the-best-ar-and-vr-headsets
3. http://resources.hwb.wales.gov.uk/VTC/ngfl/2007-08/ict/understanding-virtual-reality-imslrn/page_03.htm
4. Virtual Reality Society http://www.vrs.org.uk/virtual-reality/what-is-virtual-reality.html
5. www.google.com
6. https://www.sciencedaily.com/terms/virtual_reality.htm
7. http://www.aect.org/edtech/ed1/15/15-03.html



Mr. Kartik Nagpal [CSI- S1502687] is an IT III year student from Seth Jai Parkash Institute of Engineering and Technology(JMIT), Radaur. He can be reached at kartik.nagpal@ymail.com.

FIREWALL

Compiled by:

Geethu Nandanan and Drishya Prasad

ABSTRACT

The basic method for protecting networks today is by using a firewall: is a shield that protects the users from intruders. It offer less protection from internal attacks, due to limited firewall processing capacity, and limited support of mobile computing. Distributing a firewall to each network nodes avoids many of these problems, but weakens the security guarantees of the network. In this paper we are presenting the advantages and disadvantages of firewall and different types of firewalls. The firewall currently supports basic packet filtering and some application policies as well as secures policy distribution.

INTRODUCTION

Firewall is a network security system that detects and controls the incoming and outgoing network traffic based on fixed security rules. A firewall creates an obstacle between a trusted, secure internal network and another external network. It is used to control access between two individual systems with the help of a hardware component or software program.

Internet is a worldwide network that makes data's available to various users like home, business users and also in educational purposes. In current scenario, saving or collecting data is essential because different users build on information for various purposes. Now a days there is only a low degree of security to various networks and highly confidential information are open to everyone and it raises the degree of risk I think security and privacy are two criteria's and firewall provides a solution by protecting from vulnerable services. We must be aware about consequences and how to protect our data and critical systems when we connect to other unsecured network. An application firewall is a special firewall that is specifically structured for the type of block it is inspecting. The most widely developed application firewall is the web application firewall. The primary goal is to keep individual components secure and away from unwanted interference of external information.

TYPES

A. Packet-filtering Router

B. Application-level Gateway

C. Circuit-level Gateway

DESIGN GOALS

The ultimate goal for a firewall is to collectively sum up all the network traffic from internal to external which must go through the firewall physically trimming off all access to the local network except through the firewall. The second goal would be only commissioned traffic which is designed by the local security policy will be allowed to proceed.

Finally the last goal is that the firewall itself is resistant to infiltration inclusive is a solid authentic system with a protected operating system.

ADVANTAGES AND DISADVANTAGES

Any computer network system will have many advantages when using a firewall. They are more cheaper than securing each computer in the collective network after all there are often only one or a few firewall systems to focus on. There are some firewalls which are able to monitor viruses etc. Easy to configure or reconfigure.

The major disadvantage of firewall is that it cannot protect the network from outbreak from the inside. Firewalls cannot protect a network or Personal Computer from viruses, Trojans, worms and spyware which transmit through flash drives, portable devices etc .They may restrict commissioned users from accessing important services and do not protect against private attacks.

NEXT GENERATION FIREWALL

NGFW is a unified network platform based on hardware or software network security systems. The main goal of NGFW's is to include more OSI layer model to enhance filtering of network traffic dependent on the packet content. Also used to identify and block attacks by carry out security at application level.

TRADITIONAL FIREWALLS VS NEXT GENERATION FIREWALLS

Next-generation firewalls have developed out of our need in today's computing environments, where malware attacks have developed in elegance, depth and have found ways of apply weaknesses in traditional firewalls. Because the firewall is the first line of protection against such barrage, and also for the protection of the corporate network is of the ultimate importance, it is the reason that firewalls have derive as well to meet the risk. Where traditional firewalls have loose down is in their inefficiency to check out the data charge of network packets and their lack of grainy intelligence in differentiating other kinds of web traffic. With most network traffic using web code, traditional firewalls do not differentiate between business applications and attacks , so they must either allow or reject all of them. Something as well as traditional firewall was needed that could carry out progressive security functions without strike the inactivity of the network, this led to the development of Next generation firewall.

CONCLUSION

In current scenario, firewall technology has get significantly since the days of packet filters and network address translation .Firewall comes in different types, topologies etc.. These types and topologies help to keep that networks and internet have a protected connection between each other .Local area networks(LAN) are also ensure by firewalls which suites for the intensity of the

network .The future of firewall technology depends on the hands of today's impacts such as network security threads, viruses etc.

ACKNOWLEDGEMENTS

If words are conceded as symbols of approval and tokens of acknowledgements, then words play the heralding role of expressing our gratitude

We would like to thank our teachers who guide us by giving valuable suggestions and priceless help given to us

REFRENCE

1. Vacca, John R. (2009). Computer and information security handbook. Amsterdam: Elsevier.
2. Andrés, Steven; Kenyon, Brian; Cohen, Jody Marc; Johnson, Nate; Dolly, Justin (2004). Birkholz, Erik Pack, ed. Security Sage's Guide to Hardening the Network Infrastructure. Rockland, MA: Syngress.
3. Conway, Richard (204). Code Hacking: A Developer's Guide to Network Security. Hingham, Massachusetts: Charles River Media.
4. Andress, Jason (May 20, 2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (2nd ed.). Elsevier Science.
5. Peltier, Justin; Peltier, Thomas R. (2007). Complete Guide to CISM Certification. Hoboken: CRC Press

About the Authors:

Ms. Drishya Prasad
CSI:- 01295328
drishyaprasad1@gmail.com

Ms. Geethu Nandanan
CSI:- 01295330
geethunandan666@gmail.com

Amrita School Of Arts And Science

Department of CS & IT, Amrita School of Arts and Sciences, Kochi, Amrita VishwaVidyapeetham

SIXTH SENSE TECHNOLOGY

Compiled by:

Divya K S and Chikku janardhanan

ABSTRACT

Sixth sense technology is a wearable gesture based technology. It uses natural hand gestures to interact with information in real life. Wearable technology was introduced by Steve Mann who is considered as the father of sixth sense technology. In this paper we are discussing about the sixth generation technology and the components of the same. Sixth sense technology may change the way we look at this world now.

INTRODUCTION

Sixth sense is a wearable gestural interface technology that enhances the physical world around us with the digital information and allows us to use natural hand gestures to interact with these information. It overlap the digital world on the real world .It correlate many technologies like hand gesture recognition, image capturing etc. This concept is based on the augmented reality. We usually dont interact with the digital world directly as like we interact with the real world. The latest prototype of Sixth sense was developed by Mr. Pranav Mistry at MIT MEDIA LAB. It consists of a camera to record, a projector to display , a computing device to process and a colored sensors for identification which are insert on the fingers of a human being. Using them it facilitates us the freedom to interact with the digital world directly.

COMPONENTS NEEDED

CAMERA

It captures the picture of the object in view and tracks the user's hand gesture. The camera identifies individuals, gestures, pictures that user makes with his hand. The camera then sends this data to a smart phone for processing. In short the camera gives a digital eye which connects to the world of the digital information.

COLOURED MARKER

Colour markers are placed at the tip of the users figure so that the camera can recognize the hand gesture. Makers are made in the users figure with red yellow, blue and green colored tapes. The

arrangement and movement of these gestures are used as an interaction instruction for the application interfaces.

MOBILE COMPONENTS

The data that are sent by the camera are manipulated by a web connected smart phone. The smart phone interprets the gesture by accessing the internet with the help of the coloured markers placed in the tip of the users finger.

PROJECTOR

The interpreted information from the smart phone can be projected onto any shoal. The projector consists of a battery having 3 hours battery life and a LED projector to display the data sent by the smart phone. The downward facing projector projects the information onto a mirror.

MIRROR

The mirror is used to reflect the image onto the desired surface. It is as important as the projector, as the projector is downward facing. Thus finally the digital picture is freed from its confines and placed in the physical world.

WORKING

The working of the sixth sense technology works as the following:

Initially it captures the image of an object in view and tracks the users hand gestures. On the finger tips of the user colour markers are placed as yellow, green, red and blue tapes that helps the camera to recognize the gesture. After capturing the gesture the smart phone searches the web to interpret the hand gesture. This information that are gained through the mobile component can be projected to any surface and the image is reflected to the desired surface with the help of a mirror.

TECHNOLOGIES THAT USES SIXTH SENSE AS PLATFORM

A. Radio frequency Identification:

B. Washing machine

ADVANTAGES:

A. Portable
B. Cost Effective
C. Data access directly from the machines in real time
D. Open Source Software

CONCLUSION

The wearable technology sixth sense helps to bring the whole digital world at our finger tips. It allows the user to interact with digital data from anywhere from real time. This technology will change the way we access. It identifies the object around you and automatically displays information in the simplest way possible.

AKNOWLEDGEMENT

If words are conceded as symbols of approval and tokens of acknowledgements, then words play the important role of expressing our gratitude.

We would like to thank our teachers who guide us by giving valuable suggestions and priceless help given to us.

REFERENCES

1. "WUW – wear Ur world: a wearable gestural interface", Proceedings of CHI EA '09 Extended Abstracts on Human Factors in Computing Systems Pages 4111-4116, ACM New York, NY, USA.
2. IEEE Computer, Vol. 30, No. 2, February 1997, Wearable Computing: A First Step Toward Personal Imaging, pp25-32.
3. Cyborg, 2001.
4. Intelligent Image Processing, Wiley.
5. Elish, M. C. (2011, January). Responsible storytelling: communicating research in video demos. In Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction (pp. 25-28). ACM.

About the Authors:

Ms. Chikku Janardhanan
CSI:-01295325

zenazenar9866@gmail.com

Ms. Divya Ks
CSI:-01295326

divyakaravat@gmail.com

Department of CS & IT, Amrita School of Arts and Sciences, Kochi, Amrita Vishwa Vidyapeetham

BASIC OF NETWORKING

Compiled by:

T.Karthikeyan

INTRODUCTION:

IANA is that the non-profit organization that allocates the Internet Protocol (IP) address blocks to the Regional Internet Registries(RIRs). This RIRS manages and allocates their allotted IP address to the internet service providers and organization in their operational region. These RIRs are divided into five regions.

The IP address is that the numerical style of address which is allotted to every devices which are connected to the internet. These numerical addresses are allotted unambiguously to the connected devices. These addresses are used to uniquely identify the devices which are connected to the network. These addresses are assigned to the devices using the DHCP servers through DHCP communication between the client PC and the DHCP server.

TYPES OF ADDRESS

STATIC IP ADDRESSING

The static IP address is that the one that is permanently assigned to the device by the internet service providers which will not change even once the system is the rebooted or the IP is released manually by the user. Every time when the system is connected to the network the same IP is assigning by the ISP. These IP addresses are basically assigned to the FTP server, Web hosting Server, database and other devices wherever the same IP is required each time. The static IP address is the most reliable technique to match the domain name with their corresponding IP address using the DNS server. Since same IP address is assign to the machine, it permits the hackers to intercept the network thus extra security is to want to preventing the machine from the hackers.

DYNAMIC IP ADDRESSING

A dynamic address is an address that dynamically assign to the computer by ISP. These addresses change each time when the device is a reboot, these are assigned using the DHCP protocols. Since the ISP dynamically allocates the IP address to the networking device, it going to not invariably receive the same IP address. Even if the machine is permanently on, the dynamic IP will change when the lease time expires. Since at a regular interval of time, IP address keep changing the security is more when to compare to the static IP address. The disadvantage of using dynamic address is that it needs DHCP server to assign the address to the networking devices.

VERSION OF IP ADDRESS

IPV4

IPv4 is one among the core protocols of standards-based internetworking strategies on the internet. The IPv4 uses 32 bit (four bytes) that limits the address house by 4.2 million address. The IPv4 is classified into 5 types of classes based on the usage of the IP address among the globe.

Class
Leading bit
Start
End
Default subnet mask
CIDR notation
A
0
0.0.0.0
127.255.255.255
255.0.0.0
/8
B
10
128.0.0.0
191.255.255.255
255.255.0.0
/16
C
110
192.0.0.0
223.255.255.255
255.255.255.0
/24
D
1110
224.0.0.0
239.255.255.255
Not defined
Not defined
E
1111
240.0.0.0
255.255.255.255
Not defined
Not defined

The internet Engineering task force and IANA have some restricted usage of IP address that are used just for the special functions which are known as reserved IP address. These IP addresses are used for native networking, router table configuration, broadcasting etc.

RESERVED ADDRESS TABLE

Range
Description
0.0.0.0/8
Current network (only valid as source address)
10.0.0.0/8
Private network
100.64.0.0/10
Shared Address Space
127.0.0.0/8
Loopback
169.254.0.0/16
Link-local
172.16.0.0/12
Private network
192.0.0.0/24
IETF Protocol Assignments
192.0.2.0/24
TEST-NET-1, documentation and examples
192.88.99.0/24
IPv6 to IPv4 relay
192.168.0.0/16
Private network
198.18.0.0/15
Network benchmark tests
198.51.100.0/24
TEST-NET-2, documentation and examples
203.0.113.0/24
TEST-NET-3, documentation and examples
224.0.0.0/4
IP multicast (former Class D network)
240.0.0.0/4
Reserved (former Class E network)
255.255.255.255
Broadcast

IPV6

The IPv6 is an upgrade version of the ipv4.The most obvious improvement in IPv6 over IPv4 is that IP address is prolonged from 32 bits to 128 bits. This increase in length increases the number of IP address. The IPv6 uses the hexadecimal number to represent the address of the computer. Like IPv4, IPv6 conjointly had number of the address that is reserved for the special purpose.

TYPES OF TRANSMISSION OF DATA

UNICASTING

When using the unicasting technique, one device will send a message to precisely one device. In unicast transmission, the packet is shipped from one device to different device using LAN. Some of the common unicast application are FTP, SMTP, telnet, and FTP and this is also known as one to one communication.

BROADCAST

The broadcast is the term used to describe communication, wherever a bit of data is shipped from one source to several different destinations. The broadcast messages are supported by LAN network and all the protocols which are used for transmission. The router isn't cable of transmitting the broadcast messages whereas they have the capability to receive the broadcasted messages. And this type of transmission is known as one to many communication.

MULTICAST

In multicasting, the message is shipped to the logical cluster of a computer. It uses the internet group management protocol to spot the cluster and the cluster members. In this technique, the messages are sent from several sources and also receive by several destination devices. During multicasting, the messages are sent through the transmission medium and are received by the designated devices. This method is beneficial once a cluster of devices need a similar message at the same time from one source. This sort of transmission is known as many to many communication.

SUBNETTING

The subnetting is that the method of dividing the single network into a bunch of smaller networks. Basically, the IP address consist of two parts that's network id and also the another is host id. In subnetting the network administrators used to divide the network id into tiny fragments, so they will have many IP addresses below a similar network id. This is done by using the subnet mask. Each class of the IP address has its own subnet mask address.

Based on the use of the user we able to use the subnet mask for subnetting the IP address. During subnetting mostly, the IP address remains constant and solely the host id can vary based on the number of subnetting done.

In the on top of example, the network administrator divides the network into three completely different subnetting cluster using the subnet mask address : 141.14.22.8

REFERENCE

1. http://www.omnisecu.com/tcpip/internet-layer-ip-addresses.php
2. http://www.erg.abdn.ac.uk/users/gorry/course/intro-pages/uni-b-mcast.html
3.http://searchnetworking.techtarget.com/tip/How-to-subnet-Subnetting-calculations-and-shortcuts
4. https://www.techopedia.com/6/28587/internet/8-steps-to-understanding-ip-subnetting/5

About the Authors:

Mr. Karthikeyan. T [CSI – 01341409] is studying 3rd year B.Tech (Software Engineering) from SRM University, Kattankulathur, Kancheepuram, Tamil Nadu. His area of interest are network security, cloud security, data perturbation techniques and networking.

WIRELESS CHARGING OF MOBILE PHONES USING MICROWAVES

Compiled by:

Saniya Javed

ABSTRACT

It is a hectic task to carry everywhere the charger of mobile phones or any electronic gadget while travelling or it is very cruel when your mobile phone getting off by the time you urgently need it.

It is the major problem in today's electronic gadgets. Though the world is leading with the developments in technology, but this technology is still incomplete because of certain limitations. Today's world requires the complete technology and for this purpose we are proposing 'Wireless Charging of Mobile Phones Using Microwaves.

INTRODUCTION

Microwaves are radio waves (a form of electromagnetic radiation) with wavelengths ranging from as long as one meter to as short as one millimeter. The prefix "micro

-" in "microwave" is not meant to suggest a wavelength in the micrometer range. It indicates that microwaves are "small" compared to waves used in typical radio broadcasting, in that they have shorter wavelengths.

Figure.1: A microwave telecommunications tower on Wrights Hill in Wellington, New Zealand

Microwave technology is extensively used for point-to-point telecommunications (i.e., non broadcast uses).

Microwaves are especially suitable for this use since they are more easily focused into narrow beams than radio waves, allowing frequency reuse; their comparatively higher frequencies allow broad bandwidth and high data transmission rates, and antenna sizes are smaller than at lower frequencies because antenna size is inversely proportional to transmitted frequency. Microwaves are used in spacecraft communication, and much of the world's data, TV, and telephone communications are transmitted long distances by microwaves between ground stations and communications satellites. Microwaves are also employed in microwave ovens and in radar technology.

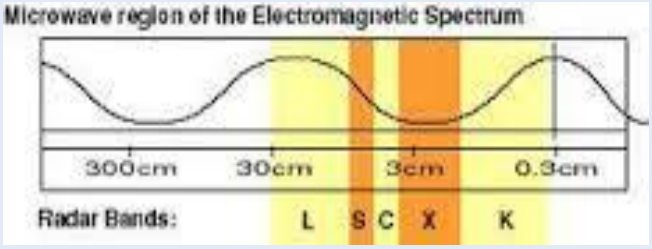
With mobile phones becoming a basic part of life, the recharging of mobile phone batteries has always been a problem. The mobile phones vary in their talk time and battery standby according to their manufacturer and batteries. All these phones irrespective of their manufacturer and batteries have to be put to recharge after the battery has drained out.

The main objective of this current proposal is to make the recharging of the mobile phones independent of their manufacturer and battery make. In this paper a new proposal has been made so as to make the recharging of the mobile phones is done automatically as you talk in your mobile phone! This is done by use of microwaves. The microwave signal is transmitted from the transmitter along with the message signal using special kind of antennas called slotted wave guide antenna at a frequency is 2.45 GHz.

There are two main concepts which of this technique, first one is electromagnetic spectrum and second is microwave region. The light contains all the regions of visible spectrum which has electromagnetic waves in it. Microwaves are radio waves which has wavelength of 1mm to 1m.The term microwaves refers to alternating current signal with frequencies between 300MHz and 300GHz.Microwave components are often distributed elements, where the phase of a voltage or current are changes significantly over the physical extent of the device because the device dimensions are on the order of the microwave wavelength. At much lower frequency, the wavelength is large enough that there is insignificant phase variation across the dimensions of the component. Microwave wavelengths range from approximately one millimeter (the thickness of a pencil lead) thirty centimeters (about twelve inches). In a microwave oven, the radio waves generated are tuned to frequencies that can be absorbed by the food. The food absorbs the energy and gets warmer. The dish holding the food doesn't absorb a significant amount of energy and stays much cooler. Microwaves are emitted from the Earth, from objects such as cars and planes, and from the atmosphere. These microwaves can be detected to give information, such as the temperature of the object that emitted the microwaves. Microwaves have wavelengths that can be measured in centimeters! The longer microwaves, those closer to a foot in length, are the waves which heat our food in a microwave oven. Microwaves are good for transmitting information from one place to another because microwave energy can penetrate haze, light rain and snow, clouds, and smoke. Shorter microwaves are used in remote sensing. These microwaves are used for clouds

and smoke, these waves are good for viewing the Earth from space Microwave waves are used in the communication industry and in the kitchen as a way to cook foods. Microwave radiation is still associated with energy levels that are usually considered harmless except for people with pace makers.

Here we are going to use the S band of the Microwave Spectrum. The frequency selection is another important aspect in transmission. Here we have selected the license free 2.45 GHz ISM band for our purpose. The Industrial, Scientific and Medical (ISM) radio bands were originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific and medical purposes. The ISM bands are defined by the ITU-T in S5.138 and S5.150 of the Radio Due to variations in national radio regulations. In recent years they have also been used for license-free error-tolerant communications applications such as wireless LANs and Bluetooth: 900 MHz band (33.3 cm) (also GSM communication in India) 2.45 GHz band (12.2 cm) IEEE 802.11b wireless Ethernet also operates on the 2.45 GHz band. Antenna gain is proportional to the electrical size of the antenna. At higher frequency more antenna gain possible, which has important consequences for miniaturized microwave systems. More bandwidth can be realized at higher frequency bandwidth is important because available frequency bands in the electromagnetic spectrum are being rapidly depleted. Microwave signals travel by line of sight and not bent by ionosphere as are low frequency signals. The effective reflection area of a radar target is proportional to targets electrical size. Molecular, atomic and nuclear reason aces occur at microwave frequency. It finds the application in the area of science remote sensing, medical diagnostics and treatment and heating methods. The majority of applications of microwave technology to communication system, radar system, environmental remote sensing and medical system. Wireless connectivity provides voice and data access to everyone, anywhere at any time. Microwave technology is extensively used for point to point communications (i.e., non broadcast uses). Microwaves are especially suitable for this use since they are more easily focused into narrow beams than radio waves; their comparatively higher frequencies allow broad bandwidth and high data flow, and also allowing smaller antenna size because antenna size is inversely proportional to transmitted frequency (the higher the frequency, the smaller the antenna size). Microwaves are the principal means by which data, TV, and telephone communications are transmitted between ground stations and to and from satellites. Microwaves are also employed in microwave oven in radar technology.



Rough plot of Earth's atmospheric transmittance (or opacity) to various wavelengths of electromagnetic radiation. Microwaves are strongly absorbed at wavelengths shorter than about 1.5 cm (above 20 GHz) by water and other molecules in the air. The microwave spectrum is usually defined as electromagnetic energy ranging from approximately 1 GHz to 100 GHz in frequency, but older usage includes lower frequencies. Most common applications are within the 1 to 40 GHz range. This is the atmospheric attenuation of microwaves in dry air with a perceptible water vapor level of 0.001 mm. The downward spikes in the graph correspond to frequencies at which microwaves are absorbed more strongly. The right half of this graph includes the lower ranges of infrared by some standards.

FUNCTIONING

The basic addition to the mobile phone is going to be the rectenna. A rectenna is a rectifying antenna, a special type of antenna that is used to directly convert microwave energy into DC electricity. Its elements are usually arranged in a mesh pattern, giving it a distinct appearance from most antennae. A simple rectenna can be constructed from a Schottky diode placed between antenna dipoles. The diode rectifies the current induced in the antenna by the microwaves.

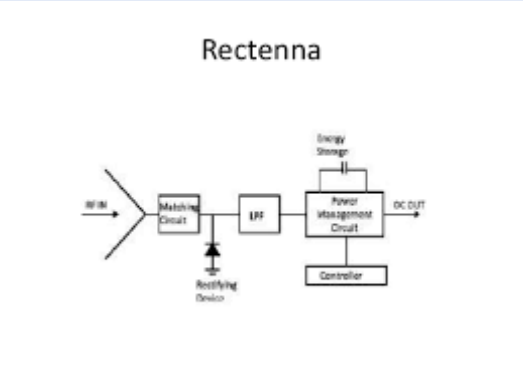
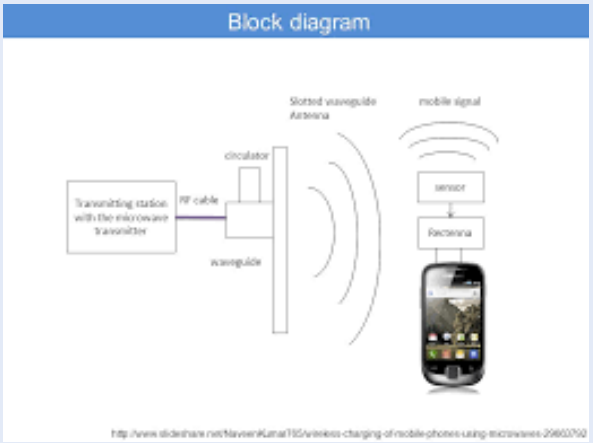


Figure 2: Rectenna

Rectenna are highly efficient at converting microwave energy to electricity. In laboratory environments, efficiencies above 90% have been observed with regularity. Some experimentation has been done with inverse rectenna, converting electricity into microwave energy, but efficiencies are much lower--only in the area of 1%. With the advent of nanotechnology and MEMS the size of these devices can be brought down to molecular level. A rectenna comprises of a mesh of dipoles and diodes for absorbing microwave energy from a transmitter and converting it into electric power. Its elements are usually arranged in a mesh pattern, giving it a distinct appearance from most antennae. A simple rectenna can be constructed from a Schottky diode placed between antenna dipoles .



The diode rectifies the current induced in the antenna by the microwaves. Rectenna are highly efficient at converting microwave energy to electricity.

It has been theorized that similar devices, scaled down to the proportions used in nanotechnology, could be used to convert light into electricity at much greater efficiencies than what is currently

possible with solar cells. This type of device is called an optical rectenna. Theoretically, high efficiencies can be maintained as the device shrinks, but experiments funded by the United States National Renewable energy Laboratory have so far only obtained roughly 1% efficiency while using infrared light.

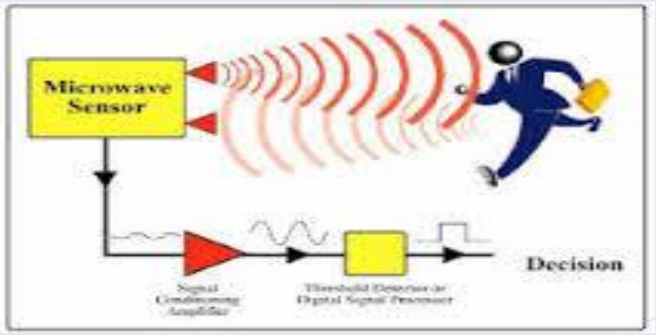


Figure 3: Sensor Circuitry

Another important component is sensor. The sensor circuitry is a simple circuit, which detects if the mobile phone receives any message signal. This is required, as the phone has to be charged as long as the user is talking. Thus a simple F to V converter would serve our purpose. In India the operating frequency of the mobile phone operators is generally 900MHz or 1800MHz for the GSM system for mobile communication.
Recentness will be used to generate large-scale power from microwave beams delivered from orbiting SPS satellites.

ADVANTAGES

Use of separate chargers is eliminated. Electricity is saved. The phone can be charged anywhere anytime. Lower risk of electrical shock because there are no exposed conductors. Easier than plugging into a power cable.

Corrosion does not occur when exposed to atmosphere. Safe for medical implants for embedded medical devices allows recharging through skin rather than having wires penetrate through skin. It does not require wire for charging

LIMITATIONS

The Mobile Handset should additionally have a device, “Rectenna” which would make it bulky and hence device size up to molecular level is essential.

The main disadvantages of wireless charging are its lower efficiency and increased resistive heating in comparison to direct contact. Implementations using lower frequencies or older drive

Technologies charge more slowly and generate heat within most portable electronics. Due to the lower efficiency, devices can take longer to charge when supplied power is equal.

INDUCTIVE CHARGING

Though some Handsets on the market currently provide wireless charging, the technology is not exactly same as mentioned here. For charging, phones are required to keep near the Charging Plate. It uses inductively coupled power transfer system.

A transmitter coil is positioned at the bottom (L1) and the receiver coil (L2) is situated at the top and these coils are embedded into different electrical devices. L1 would be the Nokia Wireless Charging Plate and L2 would be the Nokia Lumia 920, for example. In coming days, Microwave might fix various issues in the current system.

CONCLUSION

Thus this paper successfully demonstrates a novel method of using the power of the microwave to charge the mobile phones without the use of wired chargers. Thus this method provides great advantage to the mobile phone users to carry their phones anywhere even if the place is devoid of facilities for charging. A novel use of the rectenna and a sensor in a mobile phone could provide a new dimension in the revelation of mobile phone. In this modern generation where we prefer the most efficient gadgets to serve our purposes not even a slightly deviated device is acceptable. The highly accomplished cell phone sensor created by the exactly topnotch manufacturers in the industry befit your needs the best way and proves to be highly effective tools to combat security breach. Depending on the features they offer, these are available in different price ranges, you can buy the one that suits you the best.

REFERENCES

1. Wireless power transfer for mobile phone charging device.Olvitz.C,Vinko. D, Svedek.T.MIPRO, 2012 proceddings of 35th.intersation convention.
2. A.Kurs, A.Karalis, R.Moffat, J.D.Joannopoulos, P.Fisher and M.Soljacie “wireless power transfer via strongly coupled magnetic resonances, ”SCIENCE vol.317, July 2001.
3. B.Leanaerts and R.Puers “Inductive powering of freely moving system” sensors and acutators vol.A123 124.pp.522-530, 2006.
4. Liou, chong-yi; chi, Jung kuo, Ming lung la,Shau-gang mao Microwave symposium digest (MTT),2012 –IEEE MTT-S international.

About the Author:

Ms. Saniya Javed [CSI-01353621] is studying in III year of B.tech (IT) at I.T.S Engineering College, Greater Noida. Her areas of interest are Internet of Things, Database, programming etc. She can be reached at javedsaniya555@gmail.com. As a student, she has represented I.T.S in competitions held at various levels. Apart from above, I have keen interest in database, IoT, debates and creative writing.

Guided by: Mr. Ankur Saxena, Associate Professor, Computer Science and Engineering Department, I.T.S Engineering College, Greater Noida

iHOME AUTOMATION:

A BETTER WAY FOR HOME AUTOMATION

Compiled by:

Sachin S, Abhijith S, Renjith M Nair and Jacob V Kurian

ABSTRACT

"iHome Automation" presents a low cost and flexible home control and monitoring system using a web server, with IP connectivity for accessing and controlling devices and appliances remotely using Android based Smart phone app. The proposed system does not require a dedicated server PC with respect to similar systems and offers a novel communication protocol to monitor and control the home environment with more than just the switching functionality. To demonstrate the feasibility and effectiveness of this system, devices such as light switches, power plug, temperature sensor and current sensor have been integrated with the proposed home control system.

INTRODUCTION

A Home Automation system essentially provides the controls that allow users to change setting in lighting, fans, air conditioning, heating and sensors for moisture, proximity, pressure, temperature, fire to monitor a variety of conditions with various forms of data/video transmission.

Home automation is the use of one or more computers to control basic home functions and features automatically and sometimes remotely. An automated home is sometimes called a smart home. The wireless automation system is activated through a keypad, touch buttons, mobile, internet or any device which can connect to the internet.

The fundamental components of a well-designed home automation system include a computer (or computers) with the appropriate programming, the various devices and systems to be controlled, interconnecting cables or wireless links, a high- speed Internet connection, and an emergency backup power source for the computer, its peripherals, and the essential home systems.

Home automation is also called as domotics. Devices may be connected through a computer network to allow control by a personal computer, and may allow remote access from the internet. Through the integration of information technologies with the home environment, systems and appliances are able to communicate in an integrated manner which results in convenience, energy efficiency, and safety benefits.

THE CONCEPT OF IOT ITS BASIC CHARACTERISTICS

The IoT is a kind of intelligent system, which uses intelligent objects with perception, communication and computing ability to capture different information in physical world and interconnects the physical objects which can individually addressing. Consequently, overall perception, reliable transmission, and intelligent disposal is realized and the interconnection between people and things as well as among things is constructed [8].

According to the concept of IoT above, it can be found that IoT has three basic characteristics: comprehensive awareness, reliable transmission and intelligent processing. As the first step in IoT system, comprehensive awareness mainly using RFID, sensors and M2M terminal to get the information of the object anywhere and anytime. By the encryption, routing, communication and network security protocols, reliable transmission aims is realized with high accuracy and real-time. Intelligent processing depends on cloud computing, fuzzy recognition and other intelligent computing technology to analyze and hand mass information and pick up meaningful data to meet the different users.

SYSTEM ARCHITECTURE

The devices are physically connected to a Bluetooth sub-controller which is then accessed and controlled by the Smart phone using built-in Bluetooth connectivity. However, due to limited range of operation (maximum up to 100 m) the system is unable to cope with mobility and can only be controlled within the vicinity. Researchers have also attempted to provide network interoperability and remote access to control devices and appliances at home using home gateways.[15] introduced a Wi-Fi based home control system using PC based web server which manages the connected home devices. Similar designs have also been presented in[16-19] where a dedicated web server, database and a web page have been developed to interconnect and manage the devices with the Internet.

The disadvantages of these systems are twofold. Firstly, a high end personal computer has been utilized which not only increases the cost of installation but also increases the energy consumption. Secondly, development and hosting of web pages which also add to the cost. A GSM based communication and control for home appliances has also been presented by[20] where different AT commands are sent to the Home Mobile for controlling different appliances. The drawback of this system is that users are not provided with a graphical user interface and users have to remember different AT commands to control the connected devices.[21] proposed mobile IP based architecture and its potential applications in Smart homes security and automation without any actual deployment and testing. Lately few researchers have also presented use of Web services, Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) as an interoperable application layer to remotely access home automation systems.[22] introduced a smart home management scheme over the Ethernet network based on XML SOAP standards.

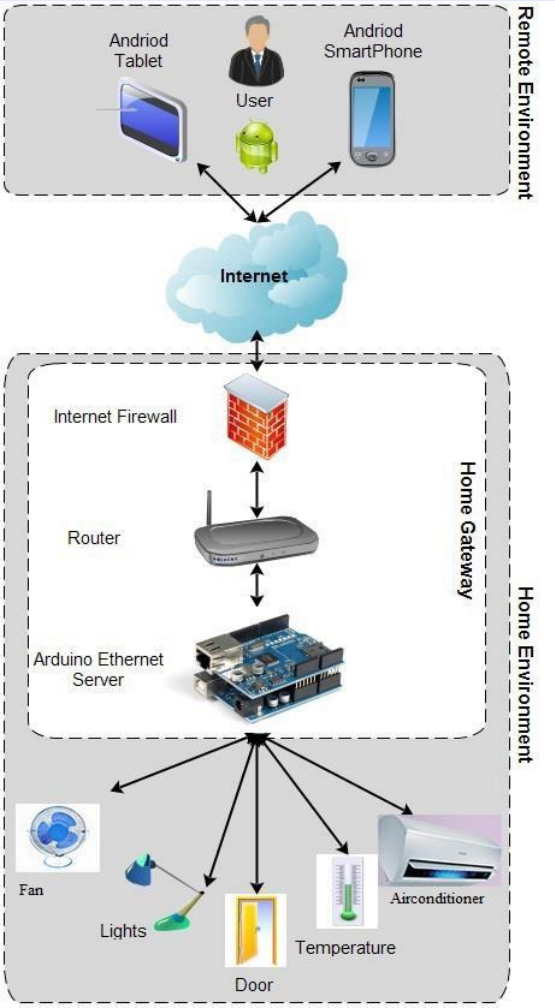


Figure 3. Architecture of proposed system

The drawback of using SOAP based Web a service is that it is complex and adds overhead to the client and server when parsing the message, resulting in slower operation and higher Bandwidth. REST [23] has been presented as a Web-based interaction for controlling household appliances using Web techniques such as HTTP caching and pushes messaging. Also a Web-based graphical user interface has been developed to manage the home devices. Home automation using Cloud computing has also been proposed by[24, 25] where users were able to control various lights and appliances within their home.

We designed and implemented a novel, standalone, flexible and low cost home controlling and monitoring system using Android app and Web services as an interoperable application layer. The system consists of a Web - server based on Arduino Ethernet, hardware interface modules and the Android compatible Smart phone app. The architecture presented in this work can be customized in different ways in order to accommodate different application scenarios with minimum recoding and design. Hence, the aim of the proposed work is not to incorporate expensive components such as high end personal computers. This system allows authorized home owners to remotely control and monitor connected devices at home using any Wi-Fi or 3G/4G enabled Smart phone which supports Java. The smart phone app provides a graphical user interface (GUI) for accessing and controlling the devices at home through server real IP.

Figure 4 shows a simplified behaviour diagram of an IoT system using MQTT. In this behaviour model, an IoT System consists of clients and brokers instantiations that interact with the final goal of enabling clients to exchange messages using a publish-subscribe pattern. Clients may publish or subscribe messages to topics, which are multi-level structures separated by a forward slash similar to a directory structure. An example of a topic for publishing GPS location information of an IoT device could be gps/device Id.

Messages can be published with a Quality of Service (QoS) parameter indicating that a message should be delivered ”at most once”, ”at least once” and

”exactly once”. MQTT also supports persistence of messages to be delivered to future clients that subscribe to a topic and will messages that are configured to be sent in specified topics when the client connection is closed abruptly. Finally, MQTT also implements keep alive messages, by means of ping request/response that are not shown in Figure

3.1.1. The MQTT V3.1 Protocol Specification [3] does not define any security management function in addition to a plain username/password authentication embedded in the connect packet.

The public review draft of MQTT V3.1.1 [9] includes a chapter with guidance only about threats and security mechanisms that should be provided by MQTT implementations. However, each MQTT implementation is free to implement or provide their own non standard version of security functions for authentication, authorization, integrity and privacy. The technical security checklist provided in the public review draft include: mutual authentication of client and servers, integrity/privacy of messages and control packages, non- repudiation of messages, and detecting malicious and abnormal behaviours of clients/servers. Mosquitto [8] is a widely adopted open source MQTT message broker that implements version 3.1.1 of the protocol, and it is the target of the work proposed in this paper.

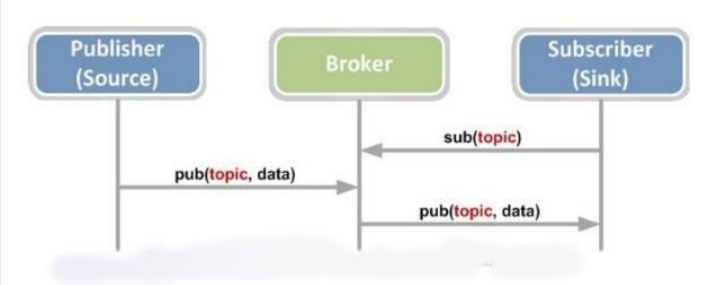


Figure 4. The publish / subscribe communication model

The non standardized security function provided by Mosquitto is nearly the same as the support provided by other open/closed source implementations (see Section VI). We performed an analysis of the authentication and usage control configuration options in the Mosquitto MQTT broker implementation from a data protection and privacy perspective. Mosquitto can be configured to allow connection by anonymous unauthenticated clients identified by a client id string, authentication using a username and password combination, and mutual client and broker authentication using Public-Key (PK) cryptography. In the configuration file it

is possible to specify the following authentication options:

- Anonymous: no authentication, identifier (id) is provided arbitrarily by client.
- Username/password: access control list with allowed clients to connect.
- Certificates (SSL/TLS): client Common Name.

(CN) from the provided certificate is used as username for access control list.

The connection with the broker is only encrypted with this authentication option, for the other options connections are in plain. The Mosquitto broker provides access control functions using static Access Control Lists (ACLs) with the possibility of giving users read and write permissions to topics. Control is limited to allow or deny subscription/publication to a topic and it is possible to use wild-cards referring to all topics in a determined path, including the client id as a variable in the path composition. This wild-card can be used, for example, to allow a client to read and write to topics where the path contains the client id and/or username used by the client for authentication in the connection to the broker (e.g., GPS based location or client id). A default access policy can be specified also for anonymous clients that do not provide an username when connecting to the broker. If the access control list is not enabled, Mosquitto does not perform access control and all clients are allowed to publish and subscribe to messages in all topics.
If the access control list is enabled the broker operates in a white-listing mode, where if no access is explicitly granted by the access control list the client is denied read and write to all topics.
Mosquitto provides a plugin mechanism to enable custom specification of authentication operations, and plugin.

CONCLUSION

Home automation is not a new industry anymore, but it is still an emerging industry in developing countries. The huge potential market leads many electronics corporation into home automation. Sony, Siemens and even Apple company are trying to share a market of home automation. But the home automation industry scale hasn't formed yet. The good and bad mixed products are together in the market. There are also no unified industry standards. It is the challenge of home automation. When compared with smart phone's history, we can find that home automation has very big chance in the future. Even five years ago, there were not so many people who owned a smart phone. It didn't have unified industry standards also.
But nowadays almost everyone has a smart phone or have used a smart phone, and Android system IOS system is becoming the standard. If the price of home automation is decreased or the practical applicability increased, there will be more people willing to buy it. So it means the production ability and technology level should improve more and more. Then it will become as popular as smart phone in the future. At last, I have to say home automation is like a rising sun. One day it will be like a burning sun bringing more decent, enjoyable and efficient life to people.

ACKNOWLEDGEMENT

WE would like to thank our anonymous reviewers for their insightful and constructive comments.

REFERENCES

1. LIU Yanbing, HU Wenping, DU Jiang. Network Information Security Architecture Based on Internet of Things [J]. ZTE Technology Journal, 2011, 17-20(01).
2. SUN Zhixin, LUO Bingqing, LUO Shengmei, ZHU Hongbo. Security Model of Internet of Things Based on Hierarchy [J].Computer Engineering, 2011,1-7(20)
3. DING Chao, YANG Lijun, WU Meng. Security Architecture and Key Technologies for IoT/CPS[J]. ZTE technology journal,2011, 11-16(01).

4. Zhang Baoquan, Zou Zongfeng, Liu Mingzheng. Evaluation on Security System of Internet of Things Based on Fuzzy-AHP Method[C].EBusiness and E- Government (ICEE), 2011 International Conference, 6-8 May 2011:1-5.
5. Pierre de Leusse, Panos Periorellis, Theo Dimitrakos, Srijith K.Nair.Self Managed Security Cell, a security model for the Internet of Things and Services[C]. First International Conference on Advances in Future Internet,2009:47-52.
6. SONG Yongguo. Brief analysis of IoT security[J]. Computer Knowledge and Technology, 2011, 2528-2530(11).
7. YAO yun. The Internet of things security model based on middleware [J]. Computer Knowledge and Technology, 2011,68-69(01).
8. WU Gongyi, WU Ying. Introduction to the Internet of things engineering [M]. Beijing: china machine press, 2012.
9. MA Ji-feng,LIANG Hao. Analysis and suggestion on information security of Internet of Things perceptual layer [J]. Modern Electronics Technique, 2012, 76-78(19).
10. REN Wei, MA Liang-li, YE Min. On M2M Technology and Its Security [J]. Netinfo Security, 2012, 6-9(07).
11. 3GPP, TS33.102, version9.2.0, 3GSeeurity, 2010, 3.
12. WU Pufeng, ZHANG Yuqing. An Overview of Database Security [J]. Computer Engineering, 2006, 85-88(12).

About the Authors:

Mr. Jacob V Kurian [CSI: 01257525], Mr. Sachin S, Mr. Abhijith S, Mr. Renjith M Nair

jacobvkurian@gmail.com

Vadakamcheril, Kodukulanji (PO), Chengannur, Alleppey, Kerala.

Call for Contributions in CSI Adhyayan

(A National Publication dedicated to IT Education, Research and Student Community)

India's IT sector continues to a trajectory of high growth since 1990s. Our education system, the prime mover of industrial growth and modern development, has seen a phenomenal growth in terms of quantity and quality - making it the third largest education system in the world after the US and China. With double digit economic growth demanding a sustained supply of knowledge workers, India has emerged as one of the world's largest consumer of education services.

India has the potential to provide the best education services with strong relationships among education, research and industry sectors.

Today, IT is a trillion dollar opportunity – so is higher education. We can proudly say that both the Indian IT and Indian ***'guru'*** are now revered globally. Both have potential and ability to scale up with global mindset. With regard to emerging technologies, they typically follow a strategy 'Start small, Grow real fast and Attempt to conquer'. In the backdrop of the above and with a view to consolidate the achievements of more than four decades of Computer Society of India (CSI) and new found vitality in education and research community, we have revived our publication of ***CSI Adhyayan*** after a gap.

CSI Adhyayan is being positioned as a nation publication dedicated for IT education, research and student community. This quarterly electronic publication performs the functions of a newsletter, a magazine and journal.

We take this opportunity to invite the contributions in this venture. Your invaluable contributions, suggestions and wholehearted support will be highly appreciated. We appeal to all our Chapters, Student Branches and member academic institutions for encouraging and motivating the students in terms of contributing innovative ideas, exploring new vistas of knowledge and new findings through CSI Adhyayan.

We especially invite news and updates from our member institutions and student branches. Please send your article to csi.adhyayan@csi-india.org.

For any kind of information, contact may be made to Dr. Vipin Tyagi via email id dr.vipin.tyagi@gmail.com.

KNOW YOUR CSI

Executive Committee (2016-17/18) »

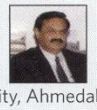
President
Dr. Anirban Basu
309, Ansal Forte, 16/2A,
Rupena Agrahara, Bangalore
Email : president@csi-india.org

Vice-President
Mr. Sanjay Mohapatra
D/204, Kanan Tower,
Patia Square, Bhubaneswar
Email : vp@csi-india.org

Hon. Secretary
Prof. A K. Nayak
Indian Institute of Business
Management, Budh Marg, Patna
Email : secretary@csi-india.org

Hon. Treasurer
Mr. R. K. Vyas
70, Sanskrit Nagar Society,
Plot No-3, Sector -14, Rohini, Delhi
Email : treasurer@csi-india.org

Immd. Past President
Prof. Bipin V. Mehta
Director, School of Computer
Studies, Ahmedabad University, Ahmedabad
Email : ipp@csi-india.org



Nomination Committee (2016-2017)

Chairman
Mr. Ved Parkash Goel
DRDO, Delhi

Dr. Santosh Kumar Yadav
New Delhi

Mr. Sushant Rath
SAIL, Ranchi

Regional Vice-Presidents

Region - I
Mr. Shiv Kumar
National Informatics Centre
Ministry of Comm. & IT, New Delhi
Email : rvp1@csi-india.org

Region - II
Mr. Devaprasanna Sinha
73B, Ekdalia Road,
Kolkata Email : rvp2@csi-india.org

Region - III
Dr. Vipin Tyagi
Jaypee University of
Engineering and Technology, Guna - MP
Email : rvp3@csi-india.org

Region - IV
Mr. Hari Shankar Mishra
Doranda, Ranchi, Jharkhand
Email : rvp4@csi-india.org

Region - V
Mr. Raju L. Kanchibhotla
Shramik Nagar, Moulali,
Hyderabad, India
Email : rvp5@csi-india.org

Region - VI
Dr. Shirish S. Sane
Vice-Principal, K K Wagh
Institute of Engg Education
& Research,Nashik, Email : rvp6@csi-india.org

Region - VII
Dr. K. Govinda
VIT University, Vellore
Email : rvp7@csi-india.org

Division Chairpersons

Division-I : Hardware
Prof. M. N. Hoda
Director, BVICAM, Rohtak Road,
New Delhi, Email : div1@csi-india.org

Division-II : Software
Prof. P Kalyanaraman
VIT University, Vellore
Email : div2@csi-india.org

Division-III : Applications
Mr. Ravikiran Mankikar
Jer Villa, 3rd Road,TPS 3, Santacruz
East Mumbai, Email : div3@csi-india.org

Division-IV : Communications
Dr. Durgesh Kumar Mishra
Prof. (CSE) & Director-MIC
SAIT, Indore Email : div4@csi-india.org

Division-V : Education and Research
Dr. Suresh C. Satapathy
ANITS, Vishakhapatnam
Email : div5@csi-india.org

an individual.

– 2 are friends.

– 3 is company.

– more than 3 makes a society. The arrangement of these elements makes the letter 'C' connoting 'Computer Society of India'.

– the space inside the letter 'C' connotes an arrow - the feeding-in of information or receiving information from a computer.

CSI Headquarter :
Samruddhi Venture Park, Unit No. 3, 4th
Floor, MIDC, Andheri (E), Mumbai-400093
Maharashtra, India
Phone : 91-22-29261700
Fax : 91-22-28302133
Email : hq@csi-india.org

CSI Education Directorate :
CIT Campus, 4th Cross Road, Taramani,
Chennai-600 113, Tamilnadu, India
Phone : 91-44-22541102
Fax : 91-44-22541103 : 91-44-22542874
Email : director.edu@csi-india.org

CSI Registered Office :
302, Archana Arcade, 10-3-190,
St. Johns Road, Secunderabad-500025,
Telengana, India
Phone : 040-27821998

Important Contact Details »

For queries, correspondence regarding Membership, contact helpdesk@csi-india.org

COMPUTER SOCIETY OF INDIA

HEAD OFFICE

Samruddhi venture park, unit no. 3, 4th Floor, MIDC,

Andheri (E) - Mumbai - 400093

Maharashtra

CONTENTS COMPILED AND EDITED BY :

DR. NILESH MODI AND DR. VIPIN TYAGI

Contact : csi.adhyayan@csi-india.org

THANKS TO MR. GHANSHYAM RAGHUWANSHI, RESERACH SCHOLAR, JAYPEE UNIVERSITY OF ENGINEERING AND TECHNOLOGY, GUNA FOR HELP IN COMPILATION.

CSI Education Directorate :

CIT Campus, 4th Cross Road, Taramani,

Chennai-600 113, Tamilnadu, India

Phone : 91-44-22541102

Fax : 91-44-22541103 : 91-44-22542874

Email : director.edu@csi-india.org