JSPM'S

BHIVRABAI SAWANT POLYTECHNIC

WAGHOLI, PUNE - 412207

SAGACITY

DEPARTMENT OF

COMPUTER ENGINEERING

Volume IV, Issue II

Published on 01/07/2019

Academic Year 2018-19

CONTENT

FIGURE INDEX

TABLE INDEX

JAYAWANT SHIKSHAN PRASARAK MANDAL's

Bhivrabai Sawant Polytechnic

(Approved by AICTE, New Delhi, Govt. of Maharashtra, Affiliated to MSBTE Mumbai)
Gat No. 720 (1&2), Wagholi, Pune-Nagar Road, Pune-412207)
Phone: 020 – 65335100 Tele fax: - + 91-020-65335100
E-mail: bspoly@rediffmail.com Website: www.jspm.edu.in

Vision and Mission of the Institute

Vision

To develop *globally* competent technocrats by imparting *quality technical education* for *socio-economic* enhancement of the nation.

Mission

M1: To nurture and maintain an environment of *high academic standard* for diploma students, encouraging higher education and entrepreneurial abilities.

M2: To deliver *quality education* by imparting basic engineering knowledge, interpersonal skills, critical thinking and creativity.

M3: To equip students with *technical skills, ethical and moral values* to meet aspirations of the society and industry to contribute sustainable development of the nation.

JAYAWANT SHIKSHAN PRASARAK MANDAL's
Bhivrabai Sawant Polytechnic
(Approved by AICTE, New Delhi, Govt. of Maharashtra, Affiliated to MSBTE Mumbai)
Gat No. 720 (1&2), Wagholi, Pune-Nagar Road, Pune-412207)
Phone: 020 – 65335100 Tele fax: - + 91-020-65335100
E-mail: bspoly@rediffmail.com Website: www.jspm.edu.in

Computer Engineering Department

Vision and Mission of the Department

Vision

To develop *technical man power* in the field of Computer Engineering to contribute the *socio-industrial* requirement.

Mission

M1: To develop *techno-savvy* engineers by imparting comprehensive Computer Engineering knowledge by innovative teaching and learning process.

M2: To develop *professional skills* committed for lifelong learning through co-curricular and extra-curricular activities.

M3: To impart *Computer Engineering education* in order to meet societal and industry needs.

JAYAWANT SHIKSHAN PRASARAK MANDAL's

Bhivrabai Sawant Polytechnic

(Approved by AICTE, New Delhi, Govt. of Maharashtra, Affiliated to MSBTE Mumbai)
Gat No. 720 (1&2), Wagholi, Pune-Nagar Road, Pune-412207)
Phone: 020 – 65335100 Tele fax: - + 91-020-65335100
E-mail: bspoly@rediffmail.com Website: www.jspm.edu.in

Computer Engineering Department

Program Educational Objectives (PEOs)

PEO 1: To bestow engineers an understanding of software and hardware systems and there applications.

PEO 2: To promote student's awareness on the lifelong learning and to introduce them to professional ethics and professional practices.

PEO 3: To develop an ability to analyze the requirement of software, understand the technical requirements design and provide novel engineering solutions.

1. GREEN COMPUTING: EFFICIENT AND ECO-FRIENDLY USE OF COMPUTER RESOURCES TO IMPROVE ENERGY UTILIZATION

RASHMI JADHAV[1], PRATIKSHA UNDRE[2]

ABSTRACT

Computers are widely used globally in business, industry, e-Agriculture, bioinformatics, medical and environmental sciences, and in every organization. Their immense application and usage requires huge amount of electricity and always lead to higher operational cost of the system. The utilization of electrical energy during working of computers generates heat as per the thermodynamics rules and therefore, air conditioners are used for providing cooling environment during working of computers and servers. Moreover, the emission of greenhouse gases such as carbon dioxide along with heat generation leads to depletion of ozone layer resulting in global warming that cause various harmful impacts on our environment and natural resources. In modern era of technology, it is also not possible to avoid the usage of computers in increasingly competitive world. Therefore, an alternative eco-friendly and cost effective technology is required in order to reduce the negative impact of computing technology on our natural resources. Green computing has emerged as eco- friendly technology for the use of computers, peripherals and servers to minimize the carbon footprint and effective use of energy. In this paper, several green initiatives currently undertaken in the computer industry to maximize energy efficiency and e-waste recycling process have been discussed. Moreover, the effective implementation of Green Computing is highlighted by minimizing the wastage of energy in small, medium and large organizations, and to promote recyclability of industrial waste.

INTRODUCTION

Green computing is the study and practice of using computing resources efficiently. The goals are similar to green chemistry i.e., to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime and promote recyclability or biodegradability of defunct products. Taking into consideration the popular use of information technology in industry, this “Green technology” should impress activists

leading to concrete action and organizational policy. Various organizations are involved in finding green technology as a way to create new profit centers while trying to help the environmental cause. The plan towards green IT should include new electronic products and services with optimum efficiency and all possible options towards energy savings Since most computers and communication systems have to run 24/7 in a cloud computing infrastructure, the energy consumption of a system is of great importance. For example, high energy consumption always leads to higher operational cost of the system. As the number of computers is increasing day by day, so is the amount of electricity consumed by them, which in turn is increasing the carbon content in the atmosphere. Moreover, high energy consumption leads to heat production and therefore more energy is required for cooling down the surrounding environment. This problem has been realized by the researchers and several corrective measures are being taken which help in minimizing the power usage of computers. For example, a user must set the power option in a computer in economic mode or the computer should go to sleep mode, when the user is not using the computer. When a user goes away from the computer for more than a few minutes, then the computer should go to stand-by mode or it may switch off automatically to use appreciable amount of energy. This paper presents several green initiatives currently under way in the computer industry, as well as issues that have been raised regarding these initiatives about the future of Green Computing.

COMPANIES USING GREEN COMPUTING TECHNOLOGY

Many companies have started manufacturing environmentally friendly products using a range of clean computing strategies. The major companies following green computing protocols are described in this section.

VIA TECHNOLOGIES

It is a Taiwanese company that manufactures motherboard chipsets, CPUs, and other computer hardware, introduced its initiative for "green computing" in 2001. With this green vision, the company has been focusing on power efficiency throughout the design and manufacturing process of its products. Its environment-friendly products are manufactured using a range of clean-computing strategies and the company is striving to educate markets on the benefits of green computing for the sake of the environment as well as productivity and overall user experience.

CARBON-FREE COMPUTING

One of the goals of VIA Technologies is to reduce the "carbon footprint" of users, the amount of greenhouse gases produced, measured in units of carbon dioxide (CO_2). Greenhouse gases naturally blanket the Earth and are responsible for its more or less stable temperature. An increase in the concentration of the main greenhouse gases i.e., carbon dioxide, methane, nitrous oxide and fluorocarbons, is believed to be responsible for Earth's increasing temperature, which could lead to severe floods and droughts, rising sea levels, and other environmental effects, affecting both life and the world's economy. VIA aims to offer the world's first PC products certified carbon free, taking responsibility for the amounts of CO_2 they emit.

Another goal of VIA's green-computing initiative is the development of energy-efficient platforms for low- power, small-form-factor (SFF) computing devices. The company works with environmental experts to calculate the electricity used by the device over its lifetime, generally three years. From this data, one can conclude how much carbon dioxide the device will emit into the atmosphere during its operation. This estimate will serve as an indicator and the company will pay regional organizations for the offsetting of the emissions. This offsetting of carbon dioxide can be achieved in different ways:

(i) One way is to plant trees that absorb CO_2 as they grow, in the region in which the processors were purchased. The necessary amount of trees per processor is represented by VIA's Tree Mark rating system.

(ii) VIA promotes the use of alternative energy sources such as solar power, so that power plants wouldn't need to burn as much fossil fuels, thereby reducing the amount of energy used.

(iii) Wetlands also provide a great service in sequestering some of the carbon dioxide emitted into the atmosphere. Although they make up only 4 to 6% of the Earth's landmass, wetlands are capable of absorbing 20 to 25% of the atmospheric carbon dioxide. VIA is working closely with organizations responsible for preserving wetlands and other natural habitats and others who support extensive recycling programs for ICT equipment. The amount paid to these organizations will be represented by a proportion of the carbon-free product's price.

(iv) In 2005, the company introduced the VIA C7-M and VIA C7 processors that

have a maximum power consumption of 20 watts (W) at 2.0 GHz and an average power consumption of one watt. These energy- efficient processors produce over four times less carbon during their operation and can be efficiently embedded in solar-powered devices.

Dell Company: Carbon emissions control has been a key issue for many companies who have expressed a firm commitment to sustainability. Dell is a good example of a company with a green image, known for its free worldwide product-recycling program. Dell's Plant a Tree for Me project allows customers to offset their carbon emissions by paying an extra $ 2 to $ 4, depending on the product purchased.

AMD: A global microprocessor manufacturer is also working toward reducing energy consumption in its products, cutting back on hazardous waste and reducing its eco-impact. The company's use of silicon-on-insulator (SOI) technology in its manufacturing and strained silicon capping films on transistors (known as - dual stress liner technology), have contributed to reduced power consumption in its products.

Intel: The world's largest semiconductor maker uses virtualization software, a technique that enables Intel to combine several physical systems into a virtual machine that runs on a single, powerful base system, thus significantly reducing power consumption.

Intel has also joined Google, Microsoft and other companies in the launch of the Climate Savers Computing Initiative that commits businesses to meet the Environmental Protection Agency's Energy Star guidelines for energy-efficient devices.

Google Inc.: With the aid of a self-styled ultra-efficient evaporative cooling technology, Google Inc. has been able to reduce its energy consumption to 50% of that of the industry average.

Advanced Power Management: It is a joint venture of Intel and Microsoft that allows a computer's BIOS to control power management functions in a computer.

STEPS FOR ADOPTION OF GREEN COMPUTING

The adoption of the following strategies will strengthen the concept and policy of green computing.

Develop a sustainable green computing plan

Discuss with the business leaders the elements that should be factored into such a plan, including organizational policies and checklists. Such a plan should include recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment. Green computing best practices and policies should cover power usage, reduction of paper consumption as well as recommendations for new equipment and recycling of old machines.

Recycling of outdated computers

Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner. Computers have toxic metals and pollutants that can emit harmful emissions into the environment [6]. Never discard computers in a landfill. Recycle them instead through manufacturer programs such as HP's Planet Partners recycling service or recycling facilities in your community or donate still-working computers to a non-profit agency.

Make environmentally sound purchase decisions

While buying a monitor, one should keep in mind one's requirements as a 17-inch monitor uses 40% more energy than a 14-inch monitor. Also, the higher the resolution, the more energy it needs. Ink-jet printers, though a little slower than laser printers, use 80 to 90% percent less energy. Thus, choice should be made wisely.

Consumers should purchase Electronic Product Environmental Assessment Tool (EPEAT) registered products. EPEAT is a procurement tool promoted by the nonprofit Green Electronics Council to help institutional purchasers evaluate, compare and select desktop computers, notebooks and monitors based on environmental attributes. It provides a clear, consistent set of performance criteria for the design of products. EPEAT recognizes manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials

Reduce paper consumption

There are many easy ways to reduce paper consumption: e- mail, electronic archiving, use the track changes feature in electronic documents, rather than redline corrections on paper. For taking print of documents, make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print

required pages.

Conserve energy

Turn off your computer when you are not going to use it for an extended period of time. Turn on power management features during shorter periods of inactivity. Power management allows monitors and computers to enter low- power states when sitting idle. Turn off the computer when the period of inactivity is more. The computer or monitor awakens from its low power sleep mode in seconds by simply hitting the keyboard or moving the mouse. Power management tactics can save energy and help protect the environment. Activating the power management features on your computer saves energy and money while helping the environment. Computer's Sleep and Hibernate settings are two of the most effective ways to make computer more environment-friendly.

- **Sleep mode:** It allows the monitor to fall asleep after idling for some time period is another easily employed method for improving energy efficiency. When a monitor falls asleep or enters a "stand by" mode, it enters a low power consumption state [7]. It saves 60-70% of electricity. The monitor screen will be blank, with no light emitting from it.
- **Hibernate mode:** The hibernate mode goes one step further than standby mode by completely powering off the computer. Invoking the hibernate mode causes the memory state to be saved onto the hard disk before powering down. When coming out of hibernate mode, the computer restores the memory state, returning the computer to its pre-hibernate state. A desktop computer will consume approximately 3 watts in hibernate mode vs 5 watts for standby. A disadvantage of the hibernate mode is that it takes slightly longer to enter and exit hibernate than standby, the result of saving and restoring the memory state to and from the disk.
- **Screen savers:** One of the simplest and most familiar power saving methods is the proper use of screen savers. The typical graphical screen saver, originally designed to minimize "burn-in" of computer monitors, actually increases power consumption rather than using a 3D graphics screen saver, and with screen burn-in no longer a concern, power use easily can be reduced by disabling screen savers. In this way, power consumed by intensive graphics is eliminated, leading to the monitor "falling asleep" after a period of idling, automatically conserving still more power. Therefore, switch off the computer and restart it again as and

when required.

- **System Standby mode:** Standby is a mode the computer, monitor, or other device enters when idles for too long. This mode helps conserve power when a computer or computer device is not in use without having to sacrifice the time it would take to turn off and on the computer. When in standby, the computer or monitor has a solid of flashing light, indicating that there is still power but the computer is in Standby. To resume, wake, or wake up a computer in Standby mode move the mouse, press a key on the keyboard, or press the power button on the computer without holding it down for more than a few seconds.

APPROACHES TO IMPLEMENT GREEN COMPUTING

Following approaches are helpful in implementation the concept of green computing. These various approaches include virtualization, power management, power supply, storage, displays, materials recycling, telecommuting, cloud computing and data compression.

Virtualization

Computer virtualization is the process of running two or more logical computer systems on one set of physical hardware. One of the primary goals of almost all forms of virtualization is making the most efficient use of available system resources. With energy and power costs increasing as the size of information technology (IT) infrastructures grow, holding expenses to a minimum is quickly becoming a top priority for many IT organizations. Virtualization has helped in that respect by allowing organizations to consolidate their servers onto fewer pieces of hardware, which can result in sizable cost savings. The data center is where virtualization can have the greatest impact and there where many of the largest companies in the virtualization space are investing their resources.

The concept originated with the IBM mainframe operating systems of the 1960s, but was commercialized for x86-compatible computers only in the 1990s. With virtualization, a system administrator could combine several physical systems into virtual machines on one single, powerful system, thereby unplugging the original hardware and reducing power and cooling consumption . Several commercial companies and open-source projects now offer software packages to enable a transition to virtual computing. Intel Corporation and AMD have also built

proprietary virtualization enhancements to the x86 instruction set into each of their CPU product lines, in order to facilitate virtualized computing.

Virtualization also fits in with the idea of "Green Computing"; by consolidating servers and maximizing CPU processing power on other servers, you are cutting costs (saving money) and taking less of a toll on our environment. Storage virtualization uses hardware and software to break the link between an application, application component, system service or whole stack of software and the storage subsystem. This allows the storage to be located just about anywhere, on just about any type of device, replicated for performance reasons, replicated for reliability reasons or for any combination of the above.

In the past, it was necessary for each computer system to have its own storage to function. Storage virtualization makes it possible for systems to access a shared storage subsystem. It also means that copies of data that are used to be stored on every computer's disks can now be stored once in the shared storage subsystem. It's clear that this approach would reduce the number of storage devices needed, the amount of power required, the heat produced and would reduce the operational and administrative costs of back up, archival storage. Since the link between the application and the actual storage device is broken by storage virtualization software, the device can be selected based upon what's most appropriate. Applications and data that are accessed frequently can be stored on high speed, expensive devices that consume more power. Applications and data that are accessed less frequently can be stored on lower speed, less expensive devices that consume less power. Rarely accessed applications and data can be migrated to archival storage devices that result in the lowest cost and require the lowest power consumption.

Power management

Power management for computer systems are desired for many reasons, particularly,

(i) to prolong battery life for portable and embedded systems

(ii) reduce cooling requirements

(iii) reduce noise, and

(v) to reduce operating costs for energy and cooling.

Moreover, lower power consumption also means lower heat dissipation, which increases system stability and less energy use, which saves money and reduces the impact on the environment.

- The Advanced Configuration and Power Interface (ACPI), an open industry standard, allows an operating system to directly control the power saving aspects of its underlying hardware. This allows a system to automatically turn off components such as monitors and hard drives after set periods of inactivity. In addition, a system may hibernate, where most components (including the CPU and the system RAM) are turned off. ACPI is a successor to an earlier Intel-Microsoft standard called Advanced Power Management, which allows a computer's BIOS to control power management functions.
- Some programs allow the user to manually adjust the voltages supplied to the CPU, which reduces both the amount of heat produced and electricity consumed. This process is called under-volting. Some CPUs can automatically under-volt the processor depending on the workload; this technology is called "Speed Step" on Intel processors, "Power Now!"/"Cool'n'Quiet" on AMD chips, Long-haul on VIA CPUs, and Long Run with Transmute processors.

  The power management for microprocessors can be done over the whole processor, or in specific areas. With dynamic voltage scaling and dynamic frequency scaling, the CPU core voltage, clock rate or both, can be altered to decrease power consumption at the price of slower performance. This is sometimes done in real time to optimize the power-performance trade off. Newer Intel Core processors support ultra-fine power control over the function units within the processors

Power supply

Power supplies in most computers aren't designed for energy efficiency. In fact, most computers drain more power than they need during normal operation, leading to higher electrical bills and a more dire environmental impact. The 80 Plus program is a voluntary certification system for power-supply manufacturers. If a PSU (Power Supply Unit) meets the certification, it will use only the power it needs at a given load. For example, if the PC requires only 20% of the total power of a 500-watt PSU, the system will consume no more than 100 watts. Only when the PC requires full power will the PSU run at the full wattage load. An 80 Plus power supply can save about 85 kilowatt hours per PC, per year. In many ways, it's the heart of a green PC, since it manages the power for all the other components. It also has the most dramatic effect on your energy bill. Moreover, all 80 Plus power supplies are also lead-free and

Ro HS compliant.

Storage capacity and performance

There are three options available, all of which vary in cost, performance and capacity. The most conventional option is the 3.5" desktop hard drive. Recently, major drive manufacturers have begun to focus on reduced power consumption, resulting in such features as the reduced RPM low-power idle mode with fixed rotation speed for reduced power consumption. The advantages of this route are the highest possible capacity, the best performance (out of the highest-end solid-state drives).

The second option, which also lends itself to affordability, is to use a 2.5" laptop hard drive. These consume less power than larger disks as a result of their smaller platters, smaller motors and firmware that is already optimized for power consumption versus most 3.5" hard disks. With capacities up to 320 GB, reasonable capacity is well within reach, although the price is substantially higher than an equivalent 3.5" disk. With a green system aimed at light use, a 120 GB or 160 GB laptop drive is a very affordable, lower-power alternative to a 3.5" disk.

The lowest power option is to use a solid state hard drive (SSD), which typically draw less than one-third the power of a 2.5" disk. The latest, highest-performance SSDs are very fast but extremely expensive and currently top out at only 64GB. That's adequate for light use, but wholly inadequate for gamers, video editing and other heavy uses. More affordable SSDs are available in larger capacities, but are not cheap and typically have slow write performance, which limits their practical utility.

Smaller form factor (e.g. 2.5 inch) hard disk drives often consume less power than physically larger drives. Unlike hard disk drives, solid-state drives store data in flash memory or DRAM. With no moving parts, power consumption may be reduced somewhat for low capacity flash based devices. Even at modest sizes, DRAM based SSDs may use more power than hard disks, (e.g., 4 GB i- RAM uses more power and space than laptop drives). Flash based drives are generally slower for writing than hard disks.

Displays on the monitors

LCD monitors typically use a cold-cathode fluorescent bulb to provide light for the display. Some newer displays use an array of light-emitting diodes (LEDs) in place of the fluorescent bulb, which reduces the amount of electricity used by the display.

LCD monitors uses three times less when active, and ten times less energy when in sleep mode. LCDs are up to 66% more energy efficient than CRTs. LCDs are also upwards of 80% smaller in size and weight, leading to fuel savings in shipping [11]. LCDs produce less heat, which means less AC will be needed to keep cool. LCD screens are also easier on the eyes. Their lower intensity and steady light pattern result in less fatigue versus CRTs. A newer LCD draws 40-60 W maximum in a modest 19", 20" or 22" size. That number grows close to 85 W or 100 W maximum for a 24" unit. Drop them down to standby or turn them off entirely when not using them to minimize power consumption. By comparison, a 21" CRT typically uses more than 120 W, more than double the power of a typical 22" LCD.

Recycling of materials

Obsolete computers are a valuable source for secondary raw materials, if treated properly, however if not treated properly they are a major source of toxic materials and carcinogens. Rapid technology change, low initial cost and even planned obsolescence have resulted in a fast growing problem around the globe. Technical solutions are available but in most cases a legal framework, a collection system, logistics and other services need to be implemented before a technical solution can be applied. Electronic devices, including audio-visual components (televisions, VCRs, stereo equipment), mobile phones and other hand-held devices and computer components, contain valuable elements and substances suitable for reclamation, including lead, copper and gold. They also contain a plethora of toxic substances, such as dioxins, PCBs, cadmium, chromium, radioactive isotopes and mercury. Additionally, the processing required reclaiming the precious substances (including incineration and acid treatments) release, generating and synthesizing further toxic by-products.

Computer recycling refers to recycling or reuse of a computer or electronic waste. This can include finding another use for the system (i.e., donated to charity) or having the system dismantled in a manner that allows for the safe extraction of the constituent materials for reuse in other products. Additionally, parts from outdated systems may be salvaged and recycled through certain retail outlets and municipal or private recycling centers.

Recycling of computing equipment can keep harmful materials such as lead, mercury and hexavalent chromium out of landfills, but often computers gathered through recycling drives are shipped to developing countries where environmental standards

are less strict than in North America and Europe. The Silicon Valley Toxics Coalition estimates that 80% of the post-consumer e-waste collected for recycling is shipped abroad to countries such as China India and Pakistan. Computing supplies, such as printer cartridges, paper and batteries may also be recycled as well.

[1] While there are several health hazards, when it comes to dealing with computer recycling some of the substances you should be aware of; (i) Lead is common in CRTs, some batteries and to some formulations of PVC. It can be harmful if not disposed of properly; (ii) Mercury is common in fluorescent tubes. With new technologies arising, the elimination of mercury in many new model computers is taking place; (iii) Cadmium is present in some rechargeable batteries. It can be hazardous to skin if exposed for too long, and (iv) Liquid crystals are another health hazard that should be taken into consideration although they do not have the nearly the same effects as the other chemicals.

Most major computer manufacturers offer some form of recycling, often as a free replacement service when purchasing a new PC. At the user's request, they may mail in their old computer, or arrange for pickup from the manufacturer. Individuals looking for environment-friendly ways in which to dispose of electronics can find corporate electronic take-back and recycling programs across the country. Open to the public (in most cases), corporations nationwide have begun to offer low-cost to no-cost recycling and have opened centers nationally and in some cases internationally. Such programs frequently offer services to take-back and recycle electronics including mobile phones, laptop and desktop computers, digital cameras and home and auto electronics. Companies offer what are called "take-back" programs that provide monetary incentives for recyclable and/or working technologies.

CONCLUSION

The tremendous growth of IT industries is slowly poisoning the environment. Green computing is an approach that can satisfy the growing demand for network computing without putting such pressure on the environment. Processor and systems could be designed which do not increase demands on the environment, but still provide an increased amount of processing capability to customers to satisfy their business needs. Now the time has come to think about the efficient use of computers and the resources, which are non-renewable. It opens a new window for the new entrepreneurs for harvesting with E-waste material and scrap computers. Green

computing is not about going out and designing biodegradable packaging for products. The features of a green computer of tomorrow would be such as energy efficiency, manufacturing and materials, recyclability, service model and self-powering. Green computer will be one of the major contributions, which will break down the 'digital divide', that separates the information rich from the information poor.

REFERENCES

[1] Soomro T.R., and Sarwar M., *"Green computing: From current to future trends".* World Academy of Science, Engineering and Technology, *Vol. 6, Issue 3, pp. 457- 460, 2012.*

[2] Garg, P., Bhatnagar, S., and Deepali, *"Green Computing"*. International Journal of Engineering Sciences, *Vol. 3, pp. 81-86, 2014.*

[3] http://www.greencomputing.co.in

[4] Harbla, A., Dimri, P., Negi, D., and Chauhan, Y. S., *"Green computing research challenges: A review",* International Journal of Advanced Research in Computer Science and Software Engineering, *Vol. 3, Issue 10, pp. 1075-1077, 2013.*

[5] Chakravarthy, V.J., and Kumar ,H., *"Green computing towards green future".* International Journal of Research in Engineering and Advanced Technology, *Vol. 1, Issue 1, 2013*.

[6] Anam A., and Syed A., *"Green computing: E-waste management through recycling"*. International Journal of Scientific and Engineering Research, *Vol. 4, Issue 5, pp. 1103-1106, 2013.*

2. IOT BASED PATIENT MONITORING SYSTEM

Kokare Pranav[1], Salunkhe Neha[2]

ABSTRACT

Health is the most important factor for human being. Hence it is essential to monitor the health parameters. For continuous monitoring the patients, there are doctors and caretaker in hospitals. But when patient returns to home. There is no facility to look after them or check the patients. Hence to overcome this problem, there is a new solution i.e. patient monitoring using IOT. Hence patient's data such as heart rate, blood pressure, temperature, ECG, position, blood oxygen etc. can be measured and sent to the server. To measure this parameters different sensors are connected to the patient's body. Then this information will be uploaded to the webpage. Doctors can access this data by typing the log in details such as user name and password. Hence continuous monitoring can be accomplished. IOT plays the major role in this system. The system we have proposed will monitor heart rate, temperature and saline level. The data will be transmitted using Wi-Fi module. We are using IOT Gecko which is an open source platform to design IOT system

INTRODUCTION

Internet provides many services for education, business, shopping, industries, social networking, entertainment, finance etc. Internet of Things is the next popular system of Internet. Using Internet of Things, we can share, communicate data with the help of webpages over internet using different protocols. The objects are connected to collect the data, analyze, used to initiate required action which provides a network to analyze, plan and decision making.

IOT is about connecting devices to the Interne and using the connection for controlling and remote monitoring of their devices. IOT is making smart network which can be controlled and planned through internet. Systems are developed with embedded technology that allows them to exchange information among each other over the internet. It is assumed that around 8 to 50 billion devices would get connected and then they will communicate by the end of 2020.

The concept of internet of Things stands on wireless network, sensors and gateway, which enables user to share communicate and then access the data or information. The IOT technology has a huge data about human, objects, time and space. By

combining the current Internet technology and IOT provides a large amount of space and smart service based on low cost sensors and wireless communication. Hence if we use Internet of Things in the area of medical, then monitoring the patients will become very easy.

COMPARISON AND CONTRAST ANALYSIS

By studying the reference papers, we found that some authors have proposed new systems and designs which are implemented to deploy IoT in the area of medical applications and healthcare. Some of the researchers follow IEEE papers to design their Internet of Things system to provide remote monitoring and emergency aid while some of the authors used other standard papers for their models. Some have just simply explained the applications of IoT in healthcare.

We present a performances, comparison and analysis of different systems in Table 1. We evaluate the proposed IoT architectures based on some parameters such as emergency aid, technology used, standards followed, and support for multi devices.

- Emergency Aid: Using IoT in the area of healthcare, the focus should be on the provision of the support in emergencies. The system must generate alarms to inform in the critical situations of patients to the doctors and their beloved ones.
- Technology: IoT supports various technologies like RFID, 3G, 4G networks GPS, GSM, GPRS, Bluetooth, zigbee, wi-fi etc. By using these technologies, one can obtain data related to person's medical status and send it

Authors	**New Architecture/ Model**	**Technology**	**Emergency Aid**	**Multi - device**	**Application**
Punit Gupta, Deepika Agrawal	No	Wi-fi, 3G, GPRS	Yes	Yes	System proposed to give proper and efficient medical services by collecting and connecting data through health status.
Abhilasha Ingole, Shrikant Ambatkar	No	Raspberry Pi, Wi-fi	No	Yes	The given system is designed for the medical data, access and store data.

Augustus E. Ibhaze, MNSE, Francis E. Idachaba	Yes	GSM, GPRS, GPS	Yes	Yes	The proposed system provides heart rate, temperature, location of patient at any time.
Prosanta Gope and Tzonelih Hwang	Yes	GPRS	Yes	Yes	Model proposed to interpret and get IOT data emergency data handling and data sharing with doctors.
Kaleem Ullah,Munam Ali Shah	Yes	RFID	No	Yes	Model proposed to provide a platform for accessing patient's health data by using smartphones and body sensors.
A.Divya, K.Keerthana, N.Kiruthikanjali,G.Nandhini and G.Yuvaraj	Yes	GSM Modem	Yes	Yes	This system is proposed to transmit the data on the webpage for regular monitoring of the patient over internet.
Meria M George,Nimmy Mary Cyriac,Sobin, Mathew,Tess Antony	Yes	Arduino, Ethernet shield	No	Yes	This model can be used for continuously monitoring using different sensors. It gives alerts using alarms in case of critical situation.
Duddela Dileep Kumar&Pratti Venkateswarlu	Yes	GSM Module	Yes	Yes	This model proposed to interprete data and to provide real time monitoring of the healthcare parameter.
Aruna Devi.S ,Godfrey Winster.S, Sasikumar.S	Yes	Wi-fi, Bluetooth	No	Yes	This system is presented to monitor real time status of the patient irrespective of the presence of doctor.

Table 2.1 Comparison And Contrast Analysis

PROPOSED SYSTEM

- In this system, we have proposed an"IoT based patient monitoring system". Now a day for the patients, who stays in home after operational days, their checking is done by medical caretaker. But sometimes if the caretaker is not with them and if sudden change occurs in wellbeing parameter, then it results in harm. Situation can become worst so, the new technology "IOT-Internet of Thing" is used. We are proposing a system with which patient can be monitor from anywhere and at any time, their family can know their health status without being with them every time. Doctor can check their status from hospital.
- In this system, the main components are microcontroller PIC16F877A, Wi-Fi module (ESP8266) and IOT Gecko.
- PIC16F877A collects the health parameter values such as heartbeats, temperature and saline level using sensors which are connected to the body of patients. Then this data is uploaded using Wi-fi module ESP8266 to the IOTGecko where we have created our own webpage for our system. Doctors will have to type the username and password and then the data can be accessed.
- IOT Gecko is a development platform where we can design IOT based system easily. We can build our own system to handle or monitor IOT system on the web. We can process sensor obtained values and display online (Webpage). IOT Gecko easily debugs IOT system and integrates it easily with desirable language with API support for all platforms.

BLOCK DIAGRAM

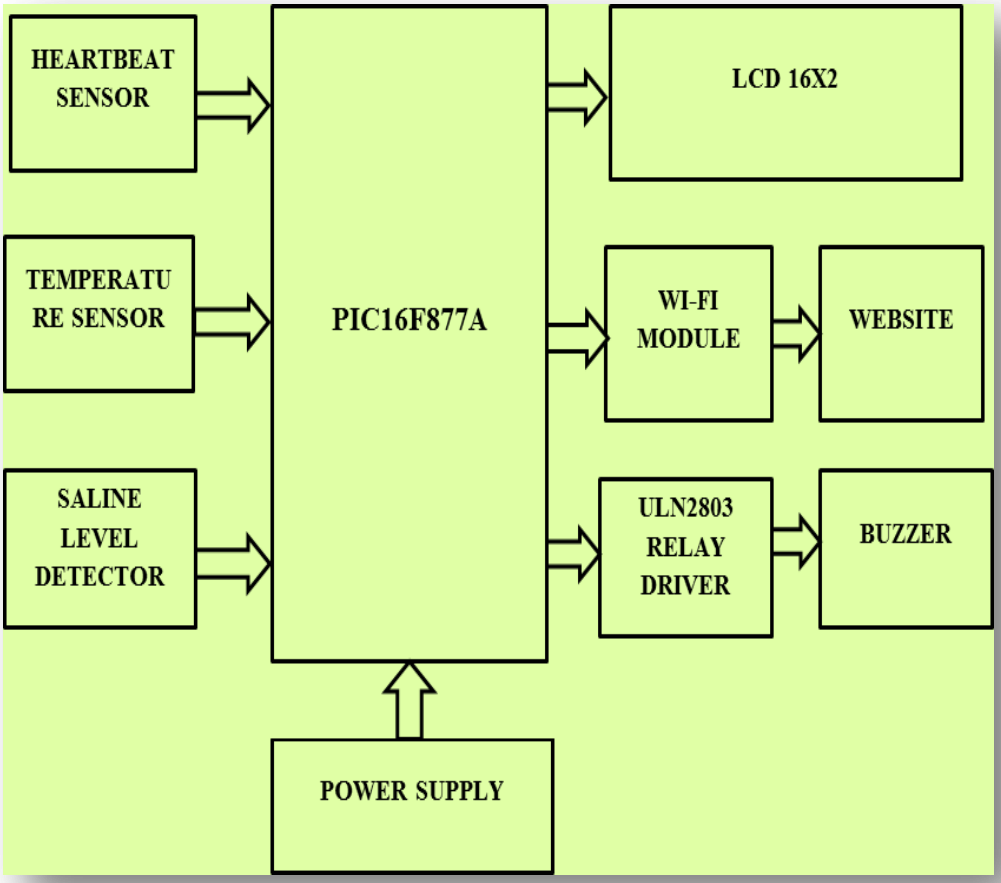

Figure 2.1: Iot Based Patient Monitoring System

CONCLUSION

This Internet of Things technology may be used to establish an architecture which can communicate over internet for the better health monitoring. IoT would be used in various fields. The more benefits can be attempted in the field of healthcare. Hence this work is done to design health care system. From the literature survey, we can conclude that the patient monitoring system using IoT can provide better accuracy and ability to continuously measure the health status in real time. Hence an improvement in the area of healthcare. With these system doctors can examine the patients from anywhere and anytime.

REFERENCES

[1]. Punit Gupta, Deepika Agrawal, Jasmeet Chhabra, Pulkit Kumar Dhir-" IoT based Smart HealthCare Kit" Jaypee University of Information Technology .Himachal Pradesh, 3.

[2]. Abhilasha Ingole, Shrikant Ambatkar, Sandeep Kakde,"Implementation of Health-care Monitoring System using Raspberry Pi", IEEE ICCSP 2015 conference., 978-1-4799-8081-9/15/$31.00 © 2015 IEEE.

[3]. Augustus E. Ibhaze, MNSE, Francis E. Idachaba, "Health Monitoring System for the Aged" 2016 IEEE, International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), 978-1- 5090-0706-6/16/$31.00 ©2016 IEEE.

[4]. Prosanta Gope and Tzonelih Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network" IEEE Sensors Journal, Vol. 16, no. 5, March 1, 2016, IEEE 1558-1748 © 2015 IEEE.

[5]. Kaleem Ullah, MunamAli,"Effective Ways to Use Internet of Things in the Field of Medical and Smart Health Care", 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things, 978-1-4673-8753-8/16/$31.00 ©2016 IEEE.

3. Designing a Selective Encryption Method Using Natural Language Processing for Text data in Mobile Ad hoc Network

Deepa Shelar[1], Kshirsagar Pratiksha[2]

ABSTRACT

In today's time security is greatly recommended for the data that is sent over the network. The research problem states, although various approaches towards security is proposed day-by-day, the security loop holes are also propagating and thus constant innovation is essential towards protection of data. The paper intends to introduce a Selective Encryption algorithm for encryption of text data which is termed as Selective Significant Data Encryption (SSDE) adding a noteworthy uncertainty to data while encryption and thus boost security. The SSDE offers adequate uncertainty to the encryption process carried out since it pick only significant data from the entire message using Natural Language Processing (NLP). As a result the encryption time is reduced and performance is improved. Symmetric key algorithms are usually competent and rapid cryptosystem over other methods, so BLOWFISH method is used for encryption. In this study, SSDE is the proposed method which is found superior to existing ones, that is, toss-a-coin and full encryption when performance is evaluated based on the extensive set of experiments done on Network Simulator.

INTRODUCTION

The world is moving towards wireless network nowadays and thus ad hoc networks are also acquiring importance. An Ad hoc network could be defined as a wireless network in which, all the nodes are able to correspond with each other directly devoid of the need of a central access point. The performance of Ad hoc network is good when less number of nodes are involved, but when the number of nodes increases, the performance gets affected and becomes difficult to manage. As mobile ad hoc networks is widely used nowadays so the security requirements for the network is also increasing which can be provided by means of cryptography.

There are two ways of keeping information secret: either hiding the existence of the information or making the information unintelligible. Cryptography could be defined

as the art and science of making the information secure from unintended audiences by encrypting it and thus making it unintelligible. The plain text is converted to cipher text while performing encryption and the cipher text is converted back to plain text in decryption. This cipher text is unintelligible to others while being transmitted in the network.

Algorithms belonging to selective encryption are admired in current state, due to the fact that they may lessen the overhead used up on data encryption or decryption that in turn enhances the efficiency of the network. This whole task is performed with the help of Natural Language Processing (NLP). NLP is associated with the area of computer science and artificial intelligence. Computational linguistics is related to computers and human languages. The approach removes the stop words from the messages and encrypts the significant data only, prior to sending over the network. The stop words are those words which are filtered out prior to or after from natural language text. They are common words which would to be of little value to the messages. The paper is ordered in the following way: Related Work is provided in section 2. Section 3 gives the concept of Selective Encryption, Proposed method SSDE is introduced in section 4, which is followed by the performance evaluation and analysis in section 5. The paper is concluded in section 6.

THE THEORY OFSELECTIVE ENCRYPTION

Selective encryption algorithms are well-liked in current circumstances due to the truth that they may decrease the overhead incurred on data encryption or decryption, and consequently advances the effectiveness of the network. Proposed work is based on the theory of selective encryption and then offers the outline of some of the selective encryption methodologies.

Selective encryption algorithms work on the principle of encrypting only specific parts of the communications and offer reliable security so as to make safe the transmitted message confidentiality. Selective encryption is capable of improving the scalability for data transmission and also trims downs the processing time. NLP is used for selective encryption of messages. Natural Language Toolkit 3.0 with python 3.5 versions is used for analyzing messages under this proposed method.

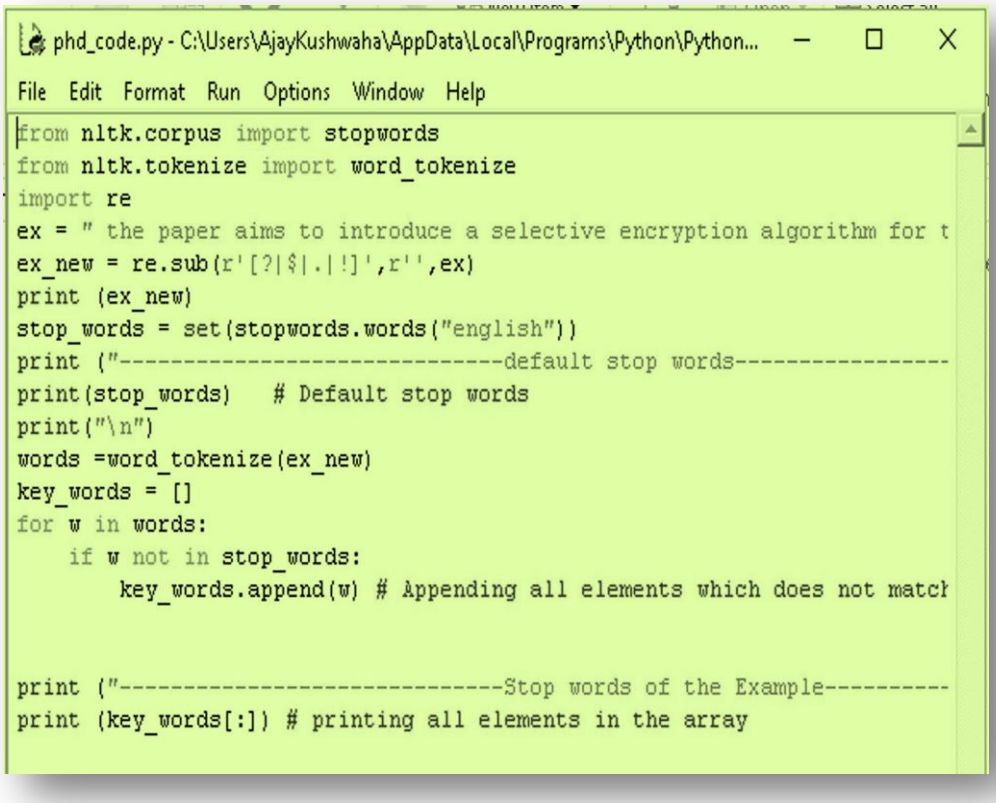

Figure 3.1: Python code along with NLTK for word processing

PROPOSED METHOD: SELECTIVE SIGNIFICANT DATA ENCRYPTION

The presented approach picks the significant data available the message and encrypts them before transferring in the network. Significant data implies the keyword that holds the meaning of entire message. Excluding significant ones, rest commonly used words like articles, pronouns, conjunctions, prepositions, and interjections are sent without encoding.Fig.2 shows the flow of data of the proposed algorithm and the various phases of selective significant data encryption.

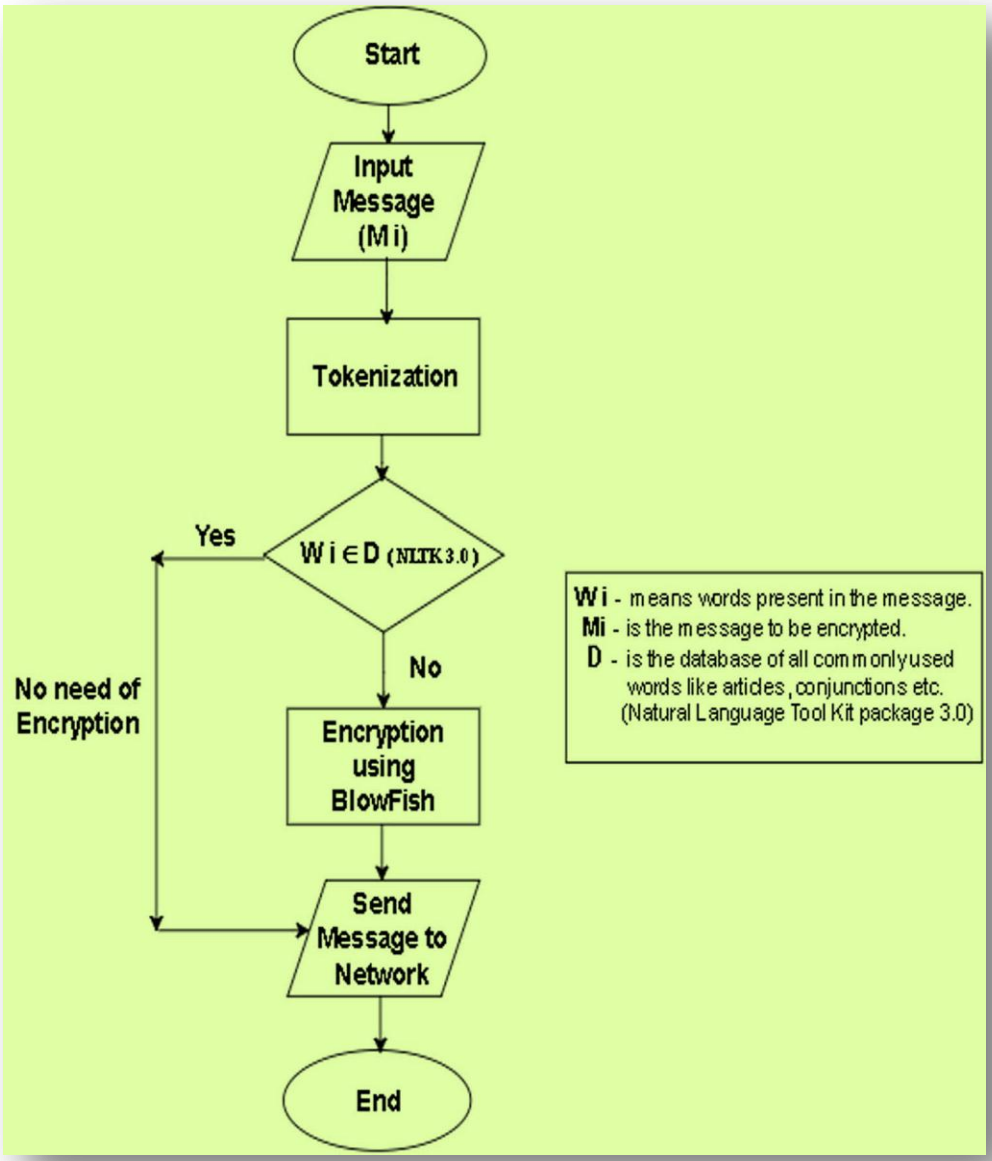

Figure 3.2: Flow chart for Selective significant data encryption

PERFORMANCE EVALUATION AND ANALYSIS

In order to examine the features of the proposed method SSDE, an extensive set of experiments are carried out within a wireless environment. In this work, the proposed method SSDE is compared with full encryption and Toss- A-Coin method. Each experiment is run for 50ns of simulation time. During the simulation experiment, the compared systems are all run under the identical scenario. The performance metrics for evaluating the SSDE are encryption time, decryption time and battery consumption.

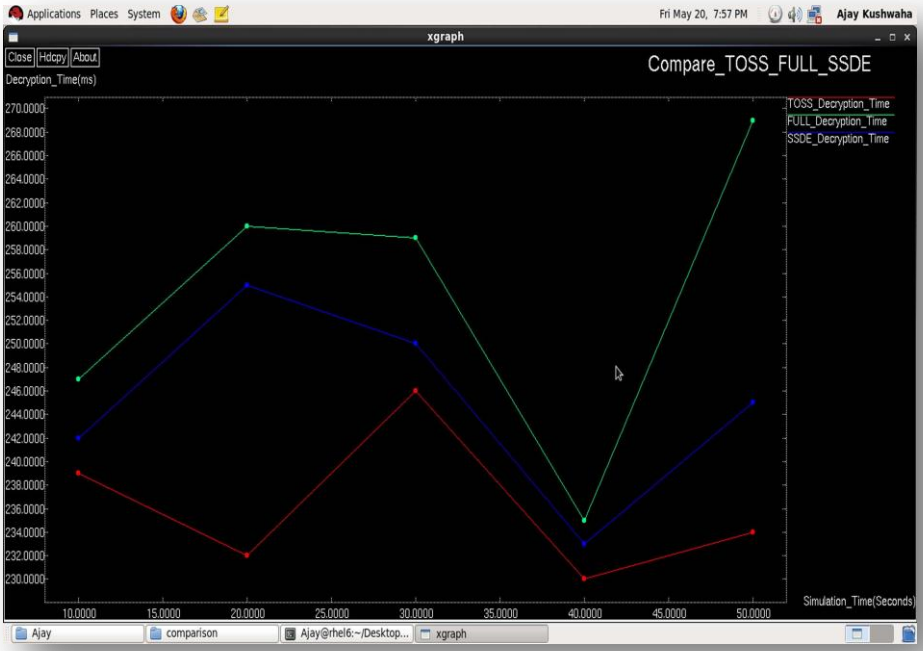

Figure 3.3 Decryption Time vs. Simulation Time

As stated earlier, two approaches are used as the comparable models with our proposed system. The first approach (i.e. full encryption) encrypts all messages without leaving any text unencrypted and thus termed as full encryption. In the second approach half of the data is encrypted and is termed as toss-a-coin method. Fig. 3 , Fig. 4 and Fig. 5 represents the comparison of decryption with simulation time , encryption with simulation time and battery consumption with simulation time respectively for the above three approaches. It can be seen from Fig. 3 that toss-a-coin and SSDE is efficient then full encryption method where as in Fig. 4 given below shows full encryption method takes more time than the other two methods (i.e. toss-a-coin and SSDE) .SSDE is encrypting the keywords (i.e. Significant words) making the intruder's task difficult; whereas toss-a-coin is less time consuming but it doesn't focuses on significant words. It encrypts random words making the intruder's task easier.

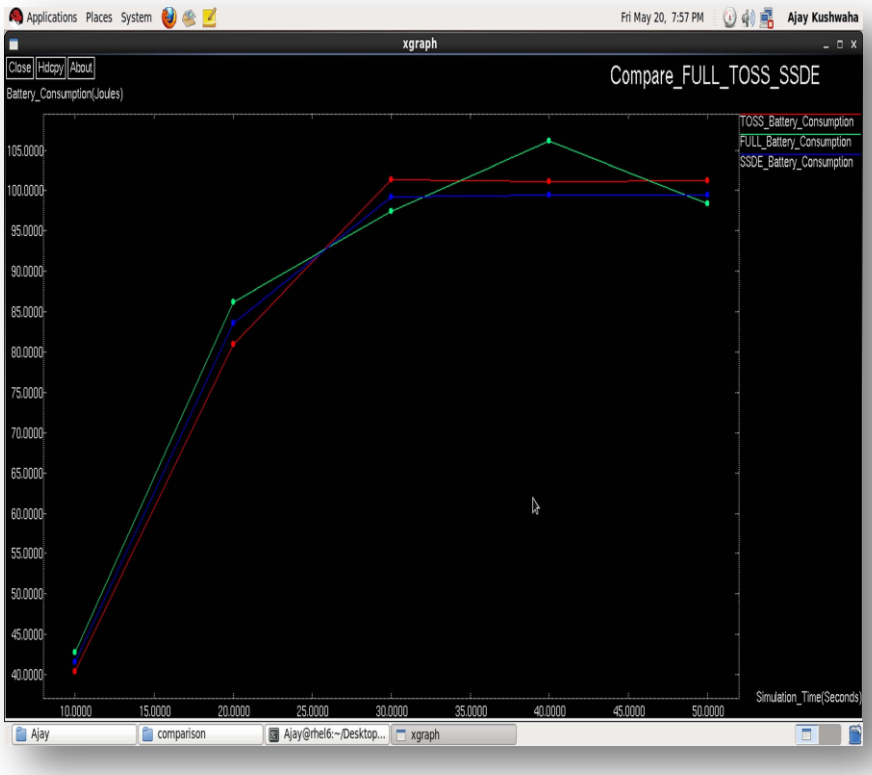

Figure 3.4: Encryption Time vs. Simulation Time

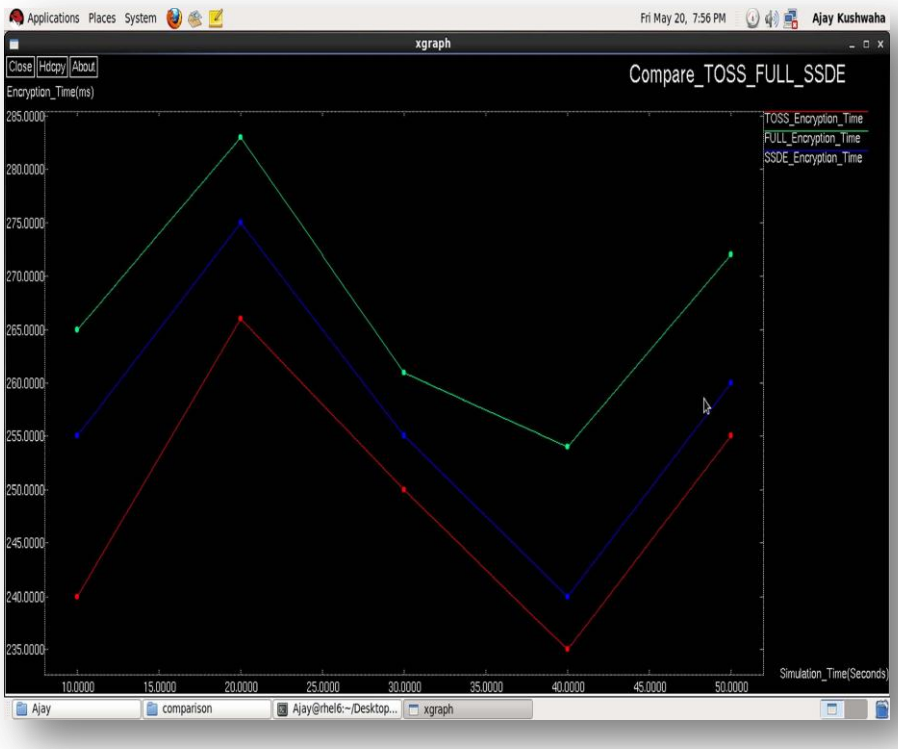

Figure 3.5: Battery Consumption vs. Simulation Time

CONCLUSION

This paper introduces a better solution for data encryption in wireless networks. The approach solution is having foundation of Selective encryption, which is one of the most capable solutions nowadays to lessen cost of data fortification as well as providing adequate uncertainty for dependability and enhanced data security. The performance of the method is evaluated based on the extensive set of experiments. The results reveal the efficiency of SSDE compared with other methods in wireless networks. Consequently the presented solution gives a viable key for securing wireless communication in Mobile Ad hoc network. This method can be used in social chatting apps, military security, corporate world communication, and government activities involving text data encryption

REFERENCES

[1] Azzedine Boukerche, Lynda Mokdad Yonglin Ren, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks," IEEE, 2011, pp. 1038- 1043.

[2] Matin M A , Hossain Md. Monir , Islam Md Foizul,Islam Muhammad Nazrul,Hossain M Mofazzal," Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN " International Conference for Technical Postgraduates (TECHPOS), at Kuala Lumpur , 14-15 Dec. 2009.

[3] Mishra Shivendra, Bhattacharjya Aniruddha," Pattern Analysis of Cipher Text : A Combined Approach", 2013 International Conference on Recent Trends in Information Technology (ICRTIT).

[4] Zhou Xin,Tang Xiaofei," Research and Implementation of RSA Algorithm for Encryption and Decryption", 2011 The 6th International Forum on Strategic Technology.

4. Secure and Authenticate Jamming Attack Proof Secure Information Transmission in Mobile Adhoc Network

Bade Pratik[1], Shinde Akash[2]

ABSTRACT

An Ad-hoc mobile network is an assembly of wireless transportable nodes devotedly creating a short-lived network lacking the use of any core-existing centralized administration or network infrastructure. MANET have restrictions owed to mobility, capability and infrastructure of mobile systems nodes because of network system as an entire. Limitations due to system or infrastructure, Limited bandwidth, Broadcast nature of communications, variable capacity link, frequent disconnections/partitions, packet loss due to transmission error. Cooperative procedures, Exposed medium, dynamically varying system topology, Inadequacy of centralized monitoring, Nothingness of clear line of opposition. There is no layered safety in MANETs like in wired network. Experimentally conclusion point out that system is fine suitable for superior and convinced data communication. Directing set of rules of Ad-hoc network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. The outcomes showed that the system throughput and security of the system is improved. This paper recommends an innovative methodology to prevent and detect the jamming based attack and equally preserve harmless the network from malicious machines. The system organization also achieved safe routing to defence MANET against malevolent machine.

INTRODUCTION

In MANET the mobile wireless network is not rely on any existed network. It is a combination of several wireless nodes that can build a network randomly. The study and growth of mobile devices and 802.1 Wi-Fi wireless networks are on demand topic of research in MANET. Ad-hoc network doesn't depend on any central supervision or constant infrastructure [such as base. Even as system nodes are moving in the system they swap the information to every other and may keep on to be in motion there and here and so the network should be prepared. Mobile system devices are not having the central control, consequently they are liberated to be in

motion, and thus the topology of such system network changes expeditiously. In the mobile Adhoc system, a number of influences such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the lifetime of a link among two mobile nodes. The superiority of service should meet the terms source system end to destination system end data packet transfer without packet loss. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multichip path. To accomplish availability and reliability network routing protocols should be prevailing compared to jamming attacks. The honesty of distribute information packets from system end to end with the help of multichip mediator nodes is a remarkable dilemma in the mobile Adhoc network. Because of the inherently self-motivated nature of the mobile system network layout, the prevailing data routes cannot be secure. Determination of information safety measures, link malfunction, exposure of malevolent node and protected information transmission within MANET is a significant tasks in any mobile network. The paper emphases on the following problem: Detection, prevention and correction of jamming attack in multipath Mobile Adhoc network and to increase performance and trustworthiness of mobile Adhoc network under jamming malicious attack with secure data transmission and routing. The main aim is to notice secure route of the mobile network, to progress the information delivery ratio and performance of MANET, to select best transmit path for safe and sound information transmission. Detection of attacks, data security, detection of malevolent node and protected information transmission in a MANET is an imperative task in mobile network. Recognition of malevolent node, data Security within a MANET is a central task in any network. The objectives are to detect jamming attacks in MANET, to prevent MANET from jamming attack, To improve the performance of network. The system proposed a secure trust value[10] which helps authenticate the system node and also remain protected the network from malicious nodes The system also perform secure routing to protect MANET against malicious node. The proposed protocol discover the jamming based attack and if original link is breakdown then new secure node is established and information is transferred from newly created link. Experimentally result showed that scheme is well suited for better data transmission. The system also perform secure routing to protect MANET against malicious node. The rest of the paper is organized as follows. Section 2 represents

literature survey related to jamming prediction, detection and failure. Section 3 provides proposed work and algorithm. Section 4 provides the implementation details of the proposed work. Section 5 concludes the paper with a summary of the work and discussion of future research directions.

PROPOSED METHOD

Determination of link failure, detection of malicious node, data safety and protected information transmission in a MANET is an imperative task in any mobile system network. The proposed algorithm is exemplified in this fragment. This algorithm provided all the steps of proposed work. The proposed algorithm will jamming based attacks in the mobile system and informed to the mobile network. The proposed algorithm discover the jamming based attack and if original link is breakdown then new secure node is established and information is transferred from newly created link. The packet drop and delivery ration is also tested to discover system performance of the network.

Algorithm

1. Threshold value setup for PDR

2. Send route request to initiate data transmission

3. Check signal strength, carrier sensing time of the requested neighbor

If all parameter tests are above threshold value then Neighbor is valid path can be established Node can transmit data to neighbor

Else if system hop sum total exceeded with initial hop then

Network is invalid

Stop transmission and Goto End

Else

Goto step 2 and make route request to another neighbor

End if

4. Check packet drop and delivery ratio of the network system Is packet delivery ratio fall to the given threshold value then Source machine arbitrarily pick out the next neighbor Is any neighbor node reply from new route excepting neighbor node then Initiate the inverse locating mechanism and direct test hello packets Read replay messages to detect jamming attack Initiate node list disagreed node onto malicious list Alarm packet is initiated

Goto Algo End If End

End Algorithm

Detect jamming attack. Initiate node list disagreed node onto malicious list alarm packet is initiated.

IMPLEMENTATION

For simulation environment used i5 2.4 GHz computer system with 8GB RAMS. The implementation script is written in TCL scripting language and a few procedures are also scripted in C++/C language. NS2 is applicable as simulation environment. In implementation scenario, simulation network used 50 system nodes, which are at random placed in unlike parts of position division with a stationary density. For this implementation scenario, simulation network parameters, transmission range, such as traffic, Dimension, Number of nodes, transmission rate, sensitivity, transmission

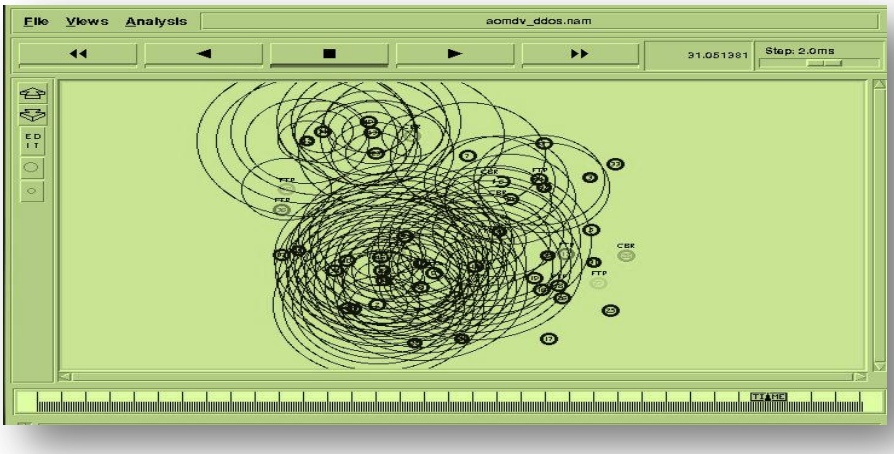

Figure 4.1: Jamming attack in network

In this Figure represents the Jamming attack in a network. Jamming attacks breakdown the network and links to the different nodes are damaged.

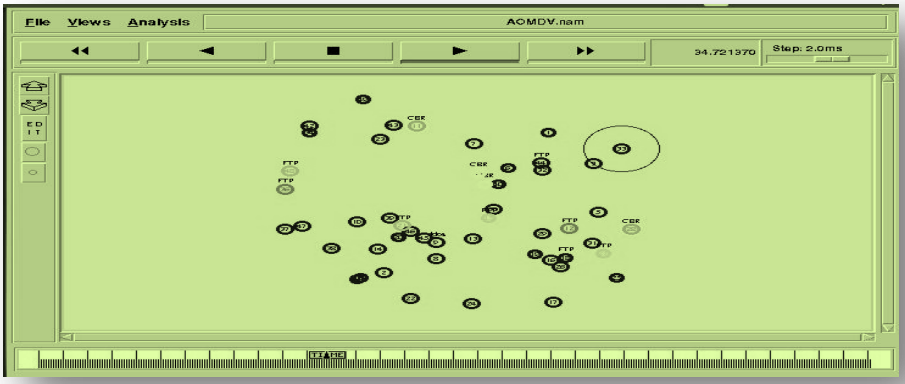

Figure 4.2: Jamming attack prevention

In this Figure represents the prevention of Jamming attack using detection node.

Figure 4.3: PDR Analysis

In this graph Packet Delivery Ratio(PDR) performance of Jamming and security

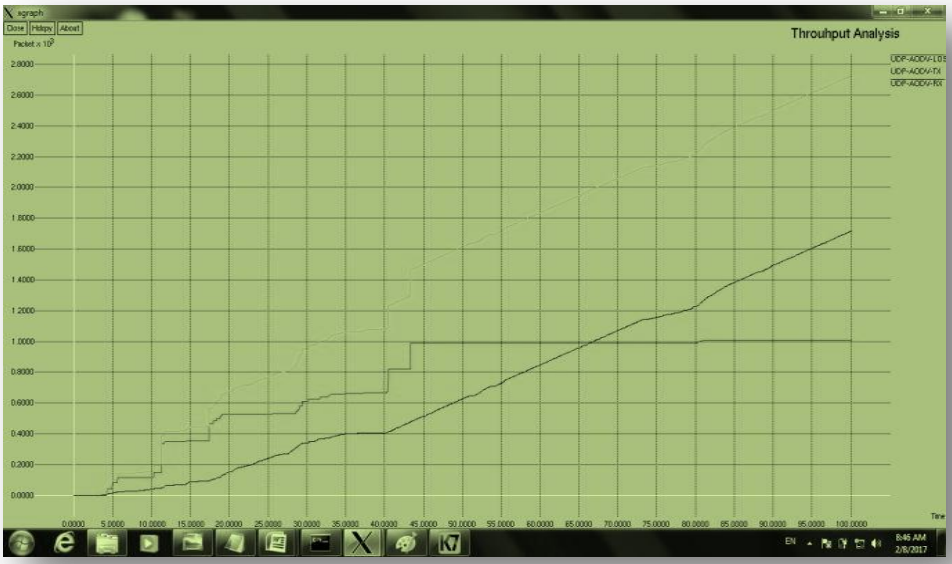

Figure 4.4: Throughput Analysis

scheme is describe in this graph. Packet sent ratio, is calculated at the node transmitter side, is the entire number of acknowledgments data packets received to the entire number of data packets communicated. By Jamming attacker technique the attacker drop of packet is humiliates the percentage ratio of data receiving. Before the attacker drop of packets is maximum and after using Jamming attacker the drop of

packets ratio is minimum.

In this graph Throughput Analysis of Jamming and Security Scheme the attacker aim is to drop the data packets or to hold the resources for that the communication is

affected. The packets forwarding capacity of jamming is a strictly increase with period of time. Overall related work the packets ratio drop is maximum and security are minimum and proposed work the packets ratio in minimum drop and and security is maximum.

CONCLUSIONS

The study and growth of mobile devices and 802.11 Wi-Fi wireless networks is on demand topic of research in MANET. Real time applications in MANET require certain QoS features, such as tolerable information loss and nominal end to end information packet interval. AODV set of regulations is a wise protocol in wireless mobile ad-hoc network. Because of the instinctively enthusiastic nature of the variable topology, the existing paths cannot be protected. MANET network using AOMDV under jamming malicious attack with secure routing and data communication. The implementation outcome revealed that the system throughput, security and system performance is enhanced. The proposed protocol discover the jamming based attack and if innovative direction is interrupted then diverse confined system node is accepted and information is communicated from freshly twisted path. The paper proposed detection and correction of jamming attack in MANET and to increase performance and trustworthiness of mobile Adhoc network under malicious assault with convinced routing and information communication. The proposed scheme is well appropriate for mobile network security. The proposed system is planning to implement in real environment and evaluate the network performance. A direction of upcoming exploration is to use better encryption scheme to secure data transmission in jamming attack.

REFERENCES

[1] Amit N Thakre, Mrs. M.Y.Joshi "Performance Analysis of AODV & DSR routing Protocol in Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network" MANETs 2010.

A. Feldmann, A. Gilbert and W. Willinger, "Data networks as cascades: Explaining the multifractural nature of internet traffic", in Proc.

ACM SIGCOMM, Sep 1998, pp.42-55

[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE 2002, pp-433-445

[3] P. Barford, J. Kline, D. Plonka, and A. Ron, " A signal analysis of network traffic anomalies", in Proc. ACM SIGCOMM Internet Meas, Workshop France, 2002, pp. 71-82.

[4] Josh Broch , David A. Maltz , David B Jhonson, Yih-chunhee, Jorjeta Jatchene, " A Performance Comparison of Multi-Hop Wireless Ad-hoc Network Routing Protocol", Computer Science Department Carnegie Mellon University Pittsburg PA 15213, Available at http://www.monarch

.cs.cmu.edu/

[5] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

5. An Android Application for Leave Sanctionation

Kulkarni Sanket[1], Kulkarni Renav[2]

ABSTRACT

This application is proposed to develop a mobile application for online leave Sanctionation system that is of importance to either an organization or an institute. This system can be used to make work automatic and to make workflow smooth of leave applications and their approvals. The regular crediting of leave is also automated. There are features like automatic credit and debit of leave, load adjustment for faculty etc. Leave Sanctionation system will reduce paper work and maintains record in more efficient way. In this Leave Sanctionation System the task for admin is it collecting requests from all employees checking their record and credit/ debit leave and send the request to superadmin. In this application HOD will have giving the permission for taking the leave. He/she can also view the leave of each and every employee. This application is most important for colleges, by using this application they can reduces paper work .The purpose of this system is, work should be done automatically. This application is online application; it is connected through data base which will maintain the records of all employees, their leaves (CO, CL, Campus,TR), working hours and all. It is very easy to use. The main aim of this application is used to reduce time

INTRODUCTION

In this leave Sanctionation system it contains activity of every day. This application can use throughout the college. Staff can submit the leave with their respective HOD. And he/she can approves that leave .It assigning Id, password to every staff while they will login to the form, because of that we can reduce the paper work. There is no chances of losing data, data will be safe and secure in this system This application can also save our time. We can adjust the leave

i.e. called load adjustment in this application.This application can be developed using android application development, because today every person has smartphone and we can access this application very easily. Now a day lot of people use android OS smartphone and it is user friendly and programmer friendly smartphone.

Existing System

The current leave sanction system it involves lots of paper work, all database are maintained manually which increases the workload of administrative section. Anew application is to be developed to ease the overall procedure and to reduce the amount of paperwork involved. In existing system every college follows manual procedure in which faculty should enter from date and to date in a application and as per that admin should do entry manually. At the end of each month Head of department will calculate leaves of every faculty member which is a time taking process and there are chance of making mistakes in manual process

Architecture.

This is the system architecture of the leave sanctionation .In this architecture shows the functionalities of the leave sanctionation. The main modules of this system are principal, HOD, staff and nonteaching staff. If the new registration is found then this will be accepted by the respective Head of Department. After the acceptance of HOD, registration will send to the respective login. After the login the particular dash board will display to the user. In the dash board all the information about user is display like no.of leaves remaining how many no.of leaves have already taken all the details are presented in this dash board. The user can first request for a leave then this leave will be sanctioned from a HOD.

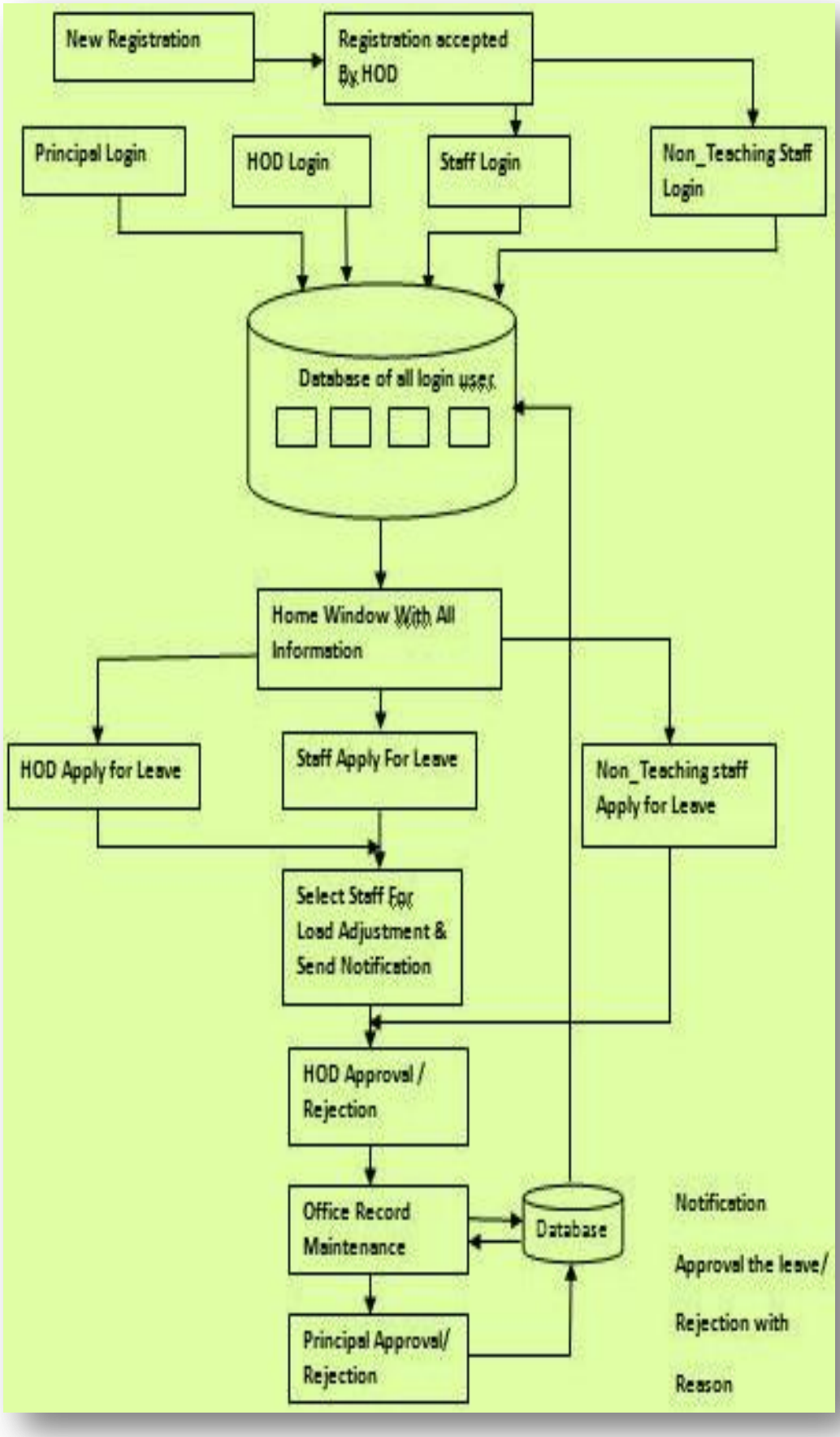

Figure 5.1: Architecture of Leave Sanctionation

The database is maintained for all login of an institute. The database is more secure which is maintaining all records. As shown in above architecture while applying request leave HOD, teaching faculty can select staff from list for adjusting load, as before taking leave it is necessary to adjust own load, so teaching faculty and HOD can select faculty for and adjust load by sending message, respective faculty can check the message and send a approval notification to requested faculty either yes or no. After load adjustment faculty can apply for leave and HOD may approve. After HOD approval from HOD The request may send to office staff. There office staff can check earlier record and update record in database for respective faculties, i.e. credit and debit of leave, and which type of leave (CO,CL,Campus,TR).

Principal approval module is last processing of request of leave applying. After office staff process the request may send to principal approval for final approval, where principal cam check load adjustment of staff and approve leave. The final approval from principal will be update in database and a notification will send to requested faculty either leave approved or not.

Dataflow Diagram

Data flow diagram means which takes input, process that input and represent output. Data flow diagram is view of system i.e. how data flow in system.

Zero Level DFD

As shown in DFD of leave sanctionation, staff can be request to apply for a leave. HOD can check request and accept or reject request of staff. After HOD approval the request send to admin for leave sanction.

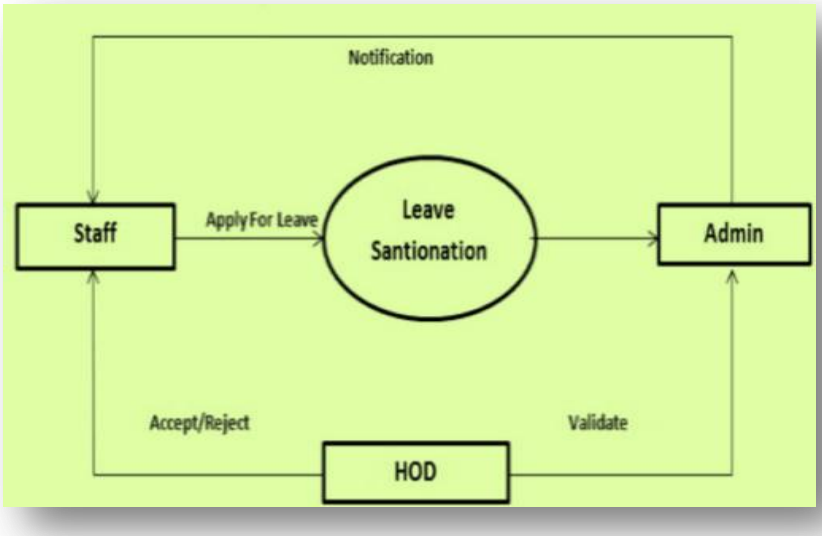

Figure 5.2: Zero Level DFD

First Level DFD

As shown in first level DFD of leave sanctionation, the staff can apply for a leave. They will register or login for a staff and then he/she can apply leave, faculty can check whether which leave type he/she will take and then faculty will apply the leave and send the leave request for particular HOD for approval.

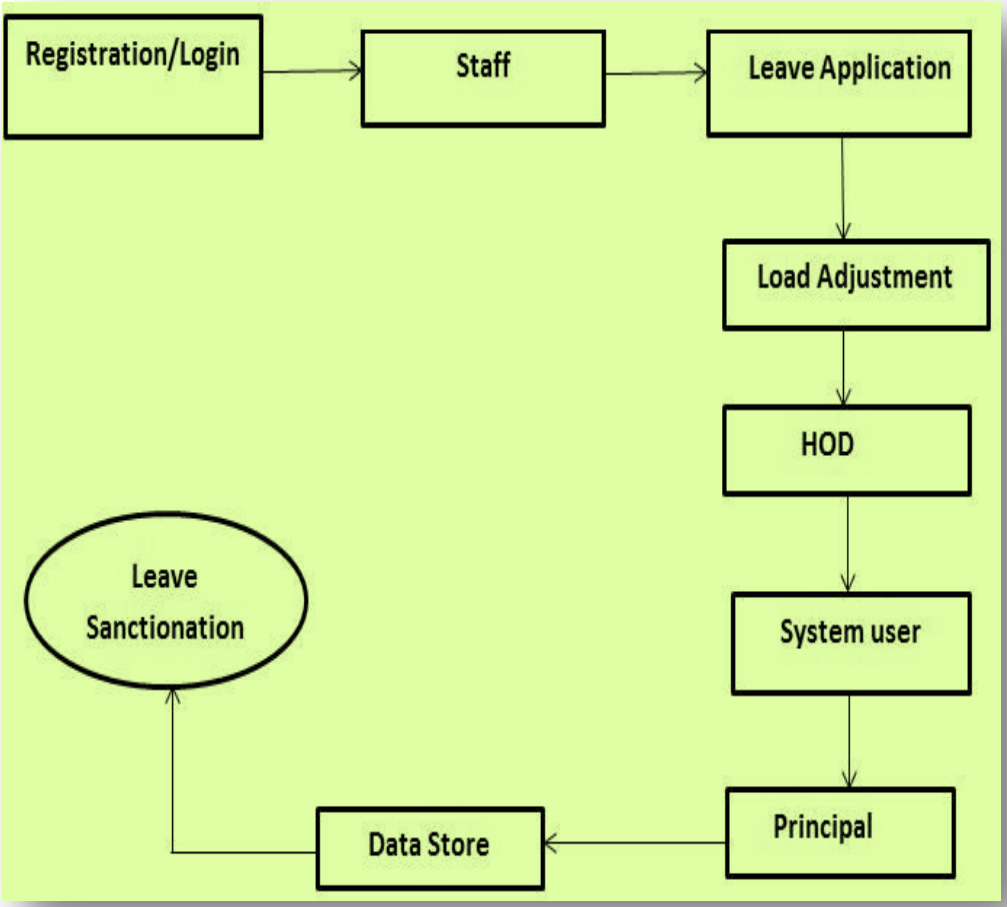

Figure 5.3: First Level DFD

Second Level DFD

As shown in second level of leave sanctionation, in this staff will login for leave application and can check the leave, and which type of leave they want they will fill the application form and update the document. After applying the leave that will send to the particular department HOD.In admin module they will able to check the details of all the staff and he also accept the leave and send leave for further processing.

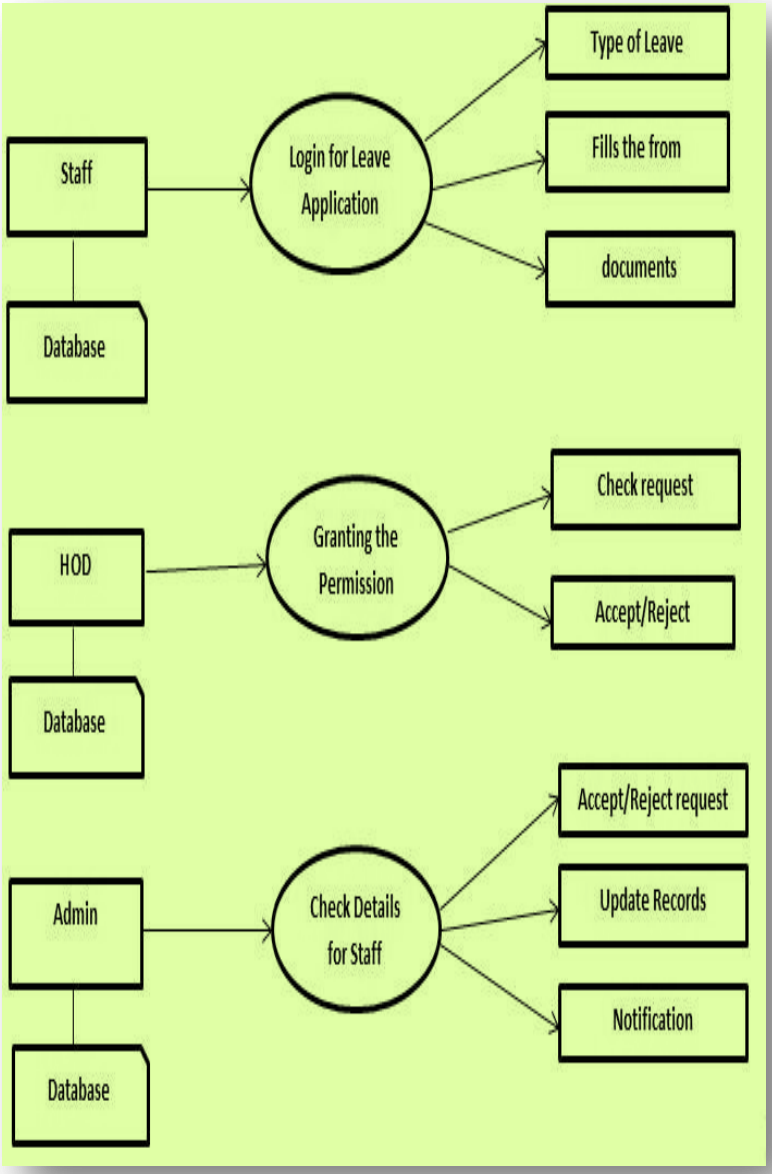

Figure 5.4: Second Level DFD

CONCLUSION

Leave sanctionation is very useful for college to maintain in the leave record of the employees. This system maintains the leave details of the staff. This application is to decrease the paper work and easier record maintenance by having the database. This approach basically deals with the record of leaves taken by faculty members and the higher authorities may accept or reject the leave applications requested by the staff.

Thus this system maintains the excess amount of job done by college to maintain the leaves.

REFERENCES

[1] Development of Employees Leave database Management System, Dama International Journal of Researchers (DIJR), ISSN: 2343-6743, *Vol 1, Issue 5, May, 2016, Page 20-38,*

[2] Leave and Payroll Management System.

Manish Singh et al.IOSR Journal of Computer Engineering (IOSR-JCE). *e-ISSN: 2278-0661,p-ISSN: 2278-8727*

[3] Mobile HRM for Online Leave Management System. A.MohanaPriya et.al. IJCSMC, *Vol. 6, Issue. 2, February 2017, pg.17 – 29*

6. SMART POLICE NAVIGATOR

Shinde Shubham[1], Lalge Akshay[2]

ABSTRACT

In recent years, mobile technology has permeated all aspects of human interaction with the world. In this paper we have discussed how to overcome the problem of communication gap between the police during their investigation. We have also discussed solution to bridge the communication gap between police and general user. We have tried to minimize the down time. This paper explains GIS based Robust Mobile application for Emergency Response System to respond to citizens under security threat with an intelligent system that can Identify the location of citizen and automatically send emergency request to nearest Policemen who has authority to resolve request falling in that area.

INTRODUCTION

In the past couple of years we have witnessed tremendous growth in mobile users all over the world as the entry of smartphones in the market at affordable prices has triggered their usage. We have experienced a major shift in the way we access the internet today with mobiles becoming the primary access point for internet usage. This latest technical advancement in the field of networking revolving around internet can be utilized to bridge the communication gap between the law enforcement agencies like police and the end users like citizens.

GIS stands for Geographical Information System. It is used for mapping, analyzing, manipulating and storing geographical data in order to provide solutions to real world problems and help in planning for the future. In this paper GIS is used to get locations and distance between co- ordinates which comes under category of analyzing GIS.

For better performance of the whole emergency system, we are using cloud for backend and database. Cloud also provides some additional benefits like security, replicas.

There are many mobile apps available for emergency response system such as "VicPD". It is one of the most successful apps for emergency response. But according to the app users there is a major fault in this app i.e fake reporting of crime. To overcome this issue we are using Aadhaar id.

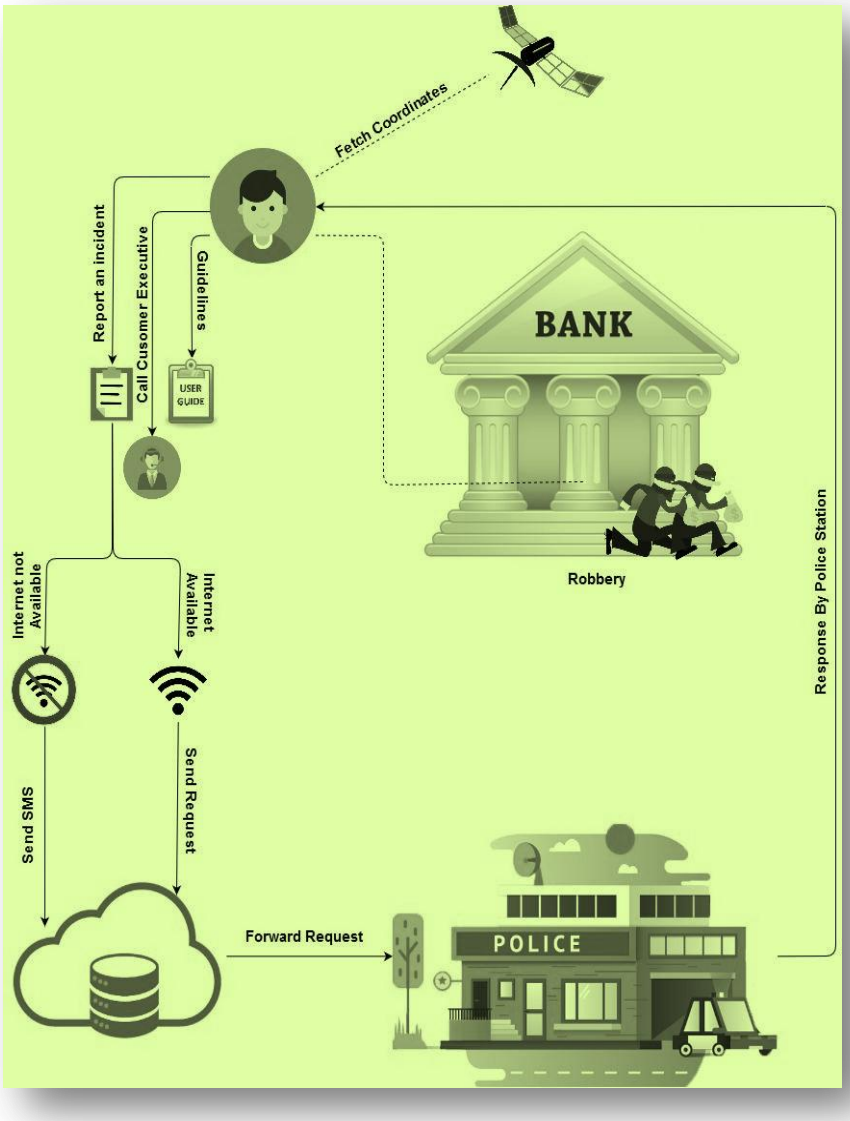

Figure 6.1: Idea of Approach

Location of user and police officials can be determined by three methods.

a) Mobile phone network: - The current cell ID can be used to identify the Base Transceiver Station (BTS) that the device is communicating with and the location of that BTS [2].

b) Satellites: - Global Positioning System (GPS) determines the device position. For using this method mobile device must be equipped with a GPS receiver [2].

Assisted-GPS (A-GPS) is a technology which shows more accurate position with consuming less battery. But disadvantage of this technology is high cost of A-GPS enabled handsets [3].

c) Short-range positioning beacons: - It is used for small areas such as a single building etc.

GENERAL USER APPLICATION

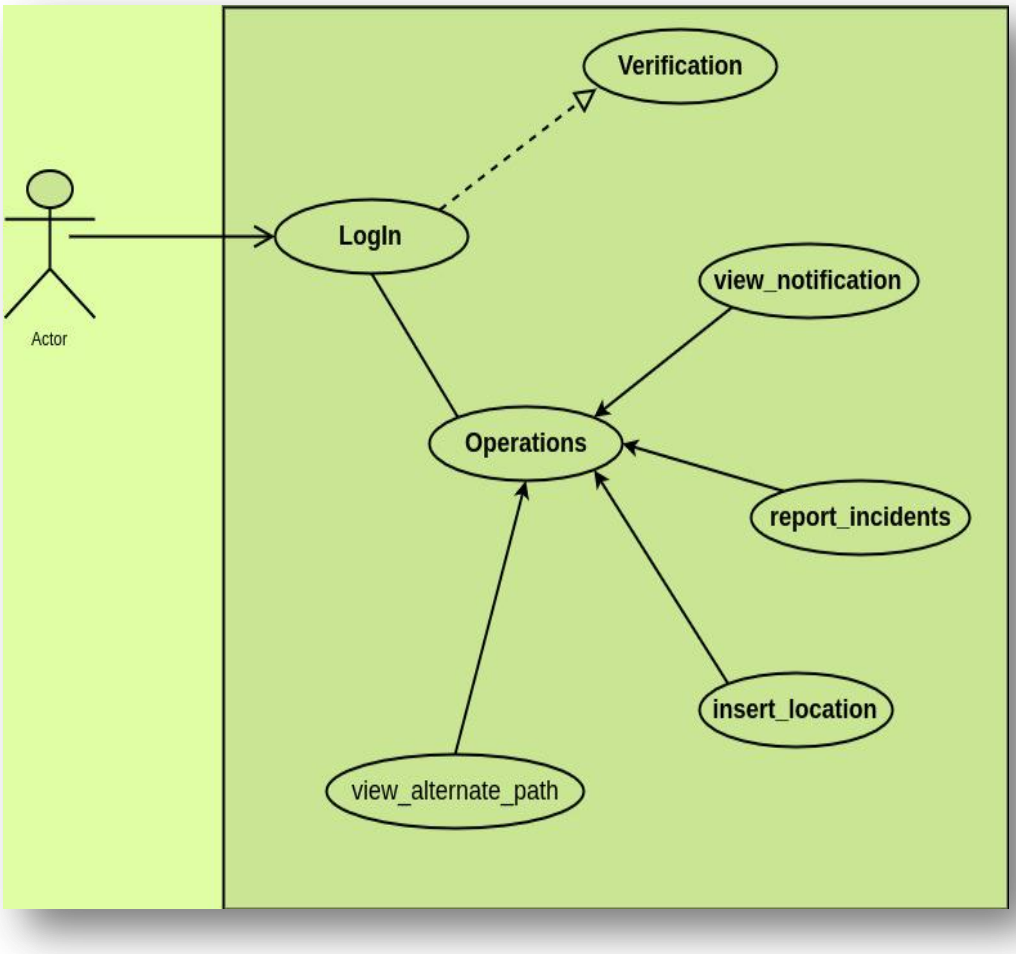

Figure 6.2: General User Application Used Case Diagram

First and foremost, the users will need to do one time registration before using the application and need to provide Aadhaar ID to avoid fake calls/request. After registration, user will be provided with the facilities like report incidents, view the notifications and popups that will contain the information such as telephone number and address of the nearby police station. Moreover, choice to view the alternate path will be provided by the police officials. User will not be given any privilege to make changes in the database but can update the action taken by the police officials. User will need to keep the GPS activated always. Physical location of the user will be tracked with the help of GPS which is inbuilt in the cellular phone. The location will be saved in the database along with the incident reported by the user. Location of the user will be tracked with the help of GPS or else we can also use google maps API [5].

POLICE APPLICATION

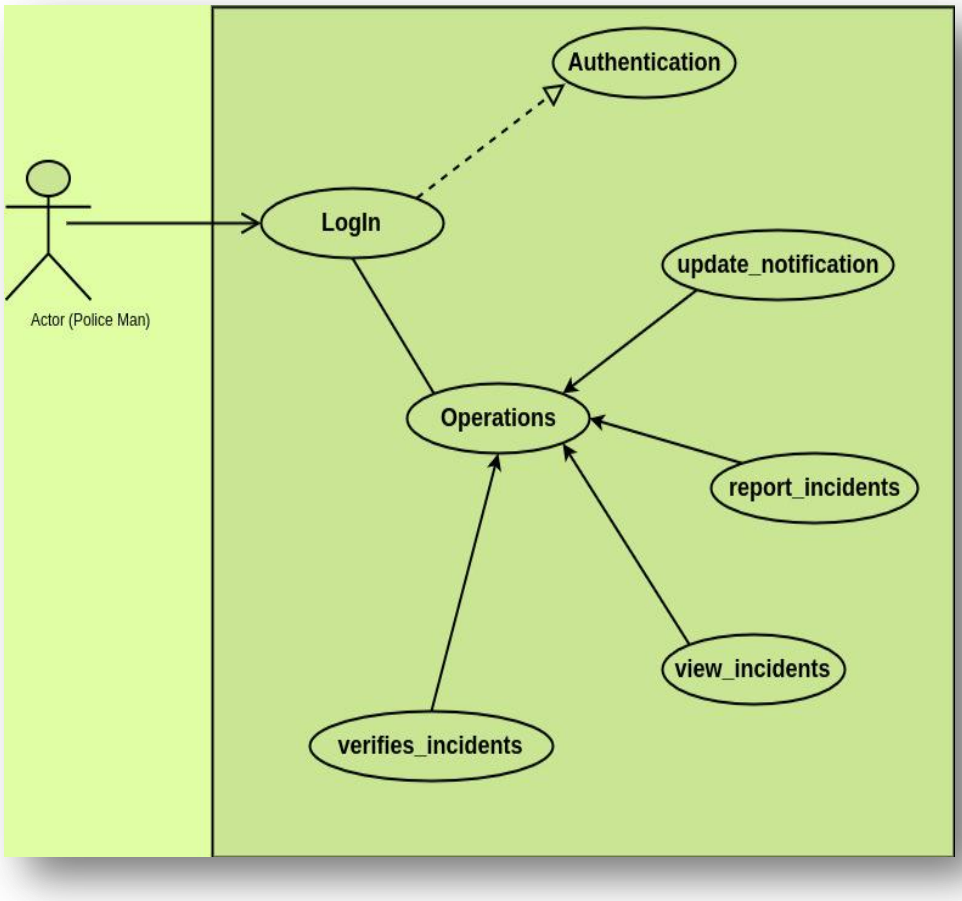

Figure 6.3: Police Application Used Case Diagram

First and foremost, the police needs to do one time registration before using the application. After registration, the police can login with the username and the password provided, as this application won't be publicly available for the general users. After logging into the application, police will be provided with the features like view user reported incidents. After the verification of the incident, the database will be updated and the notification will be broadcasted to all the users who will be using this application. Police will be given privilege to do the incident related database manipulations.

WEB PORTAL

The web app is made for police stations. It is used by station in charge to enrol all the policemen working in that station. So that in case of area problem like a policeman cannot take any actions in any other's police station area. So to resolve this issue this

portal has been made. It will let us know about police man station and then he will only get request from his area.

Other Needs of Web Portal

1. It forwards the Requests to centralized backend.
2. It also acts as a repository for all the Requests made through that station.

CLOUD

In this application, cloud will be used for storing the database to provide the facility of remote access. As mentioned in the police user application, the username and the password used by the police and users will be cross- verified with the ones stored in the database.

There are a few applications of cloud computing as Follows

Cloud computing provides dependable and secure data storage center. Cloud computing can realize data sharing between different equipment. The cloud provides nearly infinite possibility for users to use the internet. Cloud computing does not need high quality equipment for the user and it is easy to use.

SMS BOT

This SMS BOT is actually a GSM module connected on Raspberry pi. This GSM Module will work when there is no internet connectivity. It will receive a request from a user in case of no internet connectivity from user end and will transfer that request to server and after the computation of nearest policeman in that area, Server will transfer that request to nearest 5 policemen.

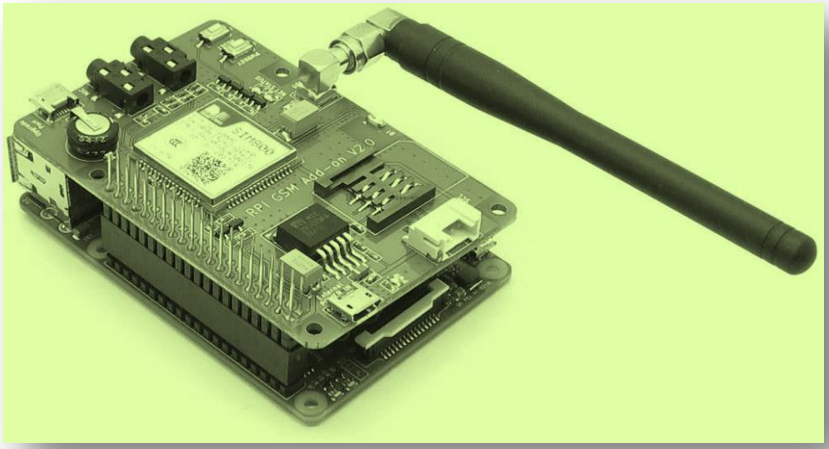

Figure 6.4: GSM Module With Raspberry pi 3.

Apart from this GSM Module there are more methods to receive request offline.

- Offline SMS API's
- Web scraping free virtual number

OFFLINE SMS API'S

There are many third party companies which provide API's for sending and receiving SMS from server But they are not that much efficient because these API's are not sending sms to server. They are actually providing the address to our server and our server is going to that address and taking that information. There are some services which are actually good but they are not providing services to Indian numbers. Till there is no availability of good third party service, So GSM module is better option.

WEB SCRAPING FREE VIRTUAL NUMBER

There are many websites which provides free virtual numbers. By using those virtual numbers we can send messages. But we cannot receive the sms to our server. In order to get message to our server we need to create scraper which will scrape that website and we will get sms on our server. If the view of website changes then scraper will not work. And data is less secure in this case. That's why we are not using this approach for sms service.

WORK FLOW

First of all, User will send a request. Which will go to the backend and backend will send request to database and take the acknowledgement. Then in backend current district of user will be found and after that all the stations will retrieve which comes under that district. Then forward request id to police station, because all police officials should know that any person is busy from their department. This portal will contain the status of policemen. Now from portal request will further go to backend. Then it will broadcast request to the nearest five policemen who will be able to handle the issues in that particular area. This will be done by the help of records inserted by police officials in web portal. And for the police app we will fetch the co-ordinates of the police under that police station which is nearest to the crime spot.If form five nearest policemen any one rejected before accepting of that request then the request will automatically formulated to sixth nearest policeman. Like this, it will go on till the request does not get a positive response. If no policeman is taking or responding to request then a dialog box will appear which will deliver call 112. If request is accepted then It will disappear from other police officials.

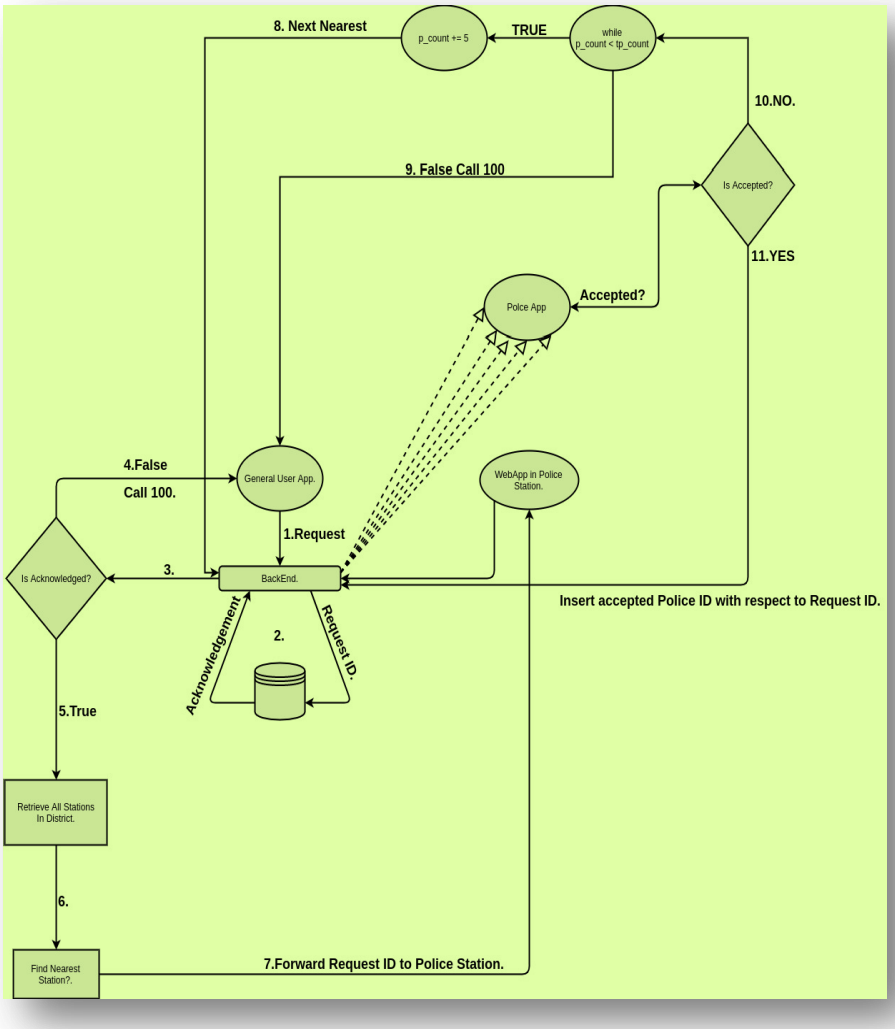

Figure 6.5: Police Application Workflow

CONCLUSION AND FUTURE WORK

In this paper we have overcome the problem of communication gap between the police during their visitation. We also provide solution to bridge the communication gap between police and general user. The problem of reporting fake crimes will be overcome as this application will need the verification through Aadhaar card. Cloud service will allow to access data remotely which will be helpful for the investigations carried by police department.

REFERENCES

[1] William Akotam Agangiba,Millicent Akotam Agangiba, *Mobile solution for Metropolitan Crime Detection and Reporting*, Journalof Emerging Trends in Computing and Information sciences, *Vol.4,*

[2] Manav Singhal, Anupam Shukla,"*Implementation of location based services in Android using GPS and Web Services*",(IJCSI) International Journal of Computer Science *Issues, Vol. 9, Issue 1, No. 2, January 2012, 1694-0814.*

7. Wi-Fi Security protocols: A survey

Chopade Rishabh [1], Avinashe Prathamesh [2]

ABSTRACT

Over the years, the wireless technology has evolved significantly and therefore the need to protect the wireless network becomes equally substantial. The choice of the best security protocol has always been an issue for the IT security staff. This paper illustrates various types of security mechanisms of wireless LAN. These security protocols are (802.11 Wired Equivalent Privacy, 802.11i Wi-Fi Protected Access and Wi-Fi Protected Access-2). The paper gives an overview of the key concepts and the working of the wireless security protocols, their limitations and the countermeasures introduced. The three protocols are also compared on the basis of the common features so as to give a deeper insight.

INTRODUCTION

Wireless networks offer a lot of benefits like scalability, flexibility, they are easy to install and also provide mobility to the devices. The data in the wireless networks is generally transmitted via radio waves which travel across the network through air, finally reaching the intended radio receiver. Since radio waves are not directional, some travel in all directions. Therefore, there arises a need to protect the data. Wireless technologies also include infrared devices like remote controls, cordless keyboards etc.

The wireless networks are classified as:

(i) **Wireless Personal Area Network (WPAN)**

This network requires low power transmission because it is a very small-scale network which covers only small local areas. Examples include mobile computing devices like PCs, wireless keyboard, mouse, PDAs The devices are usually needed to be placed in a close proximity to each other (within a several meters) for them to communicate with one another, with no infrastructure. WPAN works on the IEEE 802.15 standard. Some of the technologies used by WPAN are Bluetooth and Infrared data association

(ii) Wireless Local Area Network (WLAN)

It is a wireless network that operates within a small geographic region, such as a campus, home or a building. One such type of wireless LAN is Wi-Fi, it generally

uses 2.4GHz of frequency bands but 5GHz ISM band is also opted by users to provide additional bandwidth. Wi-Fi supports 802.11 standards.

(iii) Wireless Metropolitan Area Network (WMAN)

It is a network that provides connectivity to the users within a metropolitan area (generally a few kilometers). These networks are larger in size as compared to WLAN; therefore their functionalities also differ from each other. They establish a connection between the different buildings. Many WMANs also provides broadband access to the users in local areas

(iv) Wireless Wide Area Network (WWAN)

This network can provide connectivity to the users and the devices across large geographic areas. They are mainly used for mobile and satellite communications. WWANs include technologies like Global System for Mobile Communications (GSM), UMTS, cellular, CDMA One/CDMA2000 and Wi-Max.

WIRELESS SECURITY PROTOCOLS OVERVIEW

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was introduced in 1997 with the intention to provide security to the wireless network through encryption and checksum. WEP uses the traditional stream cipher RC4 as shown in the Figure 1. The purpose of using RC4 for WEP encryption was to provide data confidentiality and integrity with less CPU utilization and complexity

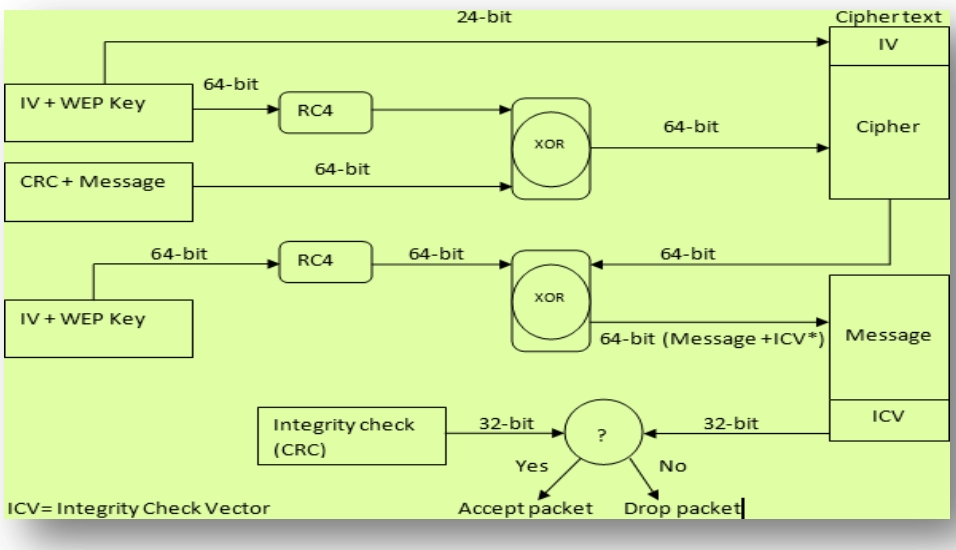

Figure 7.1: WEP working

At the time of encryption, a 40-bit master key combines with a 24-bit Initialization vector to form a 64-bit seed; it goes though the RC4 algorithm. The output of the RC4 algorithm is the random key sequences. The second input is the actual message along with its checksum, after passing both the inputs through XOR function the cipher text is generated. On the receiver's side the master key and the IV is used to decrypt the message and its checksum and calculates the checksum again.

Vulnerabilities of WEP

Although WEP was intended to be efficient, there were many flaws in technique that made it easily crack able. The problems in the RC4 algorithm are presented by Fluhrer, Mantin and Shamir in They described that WEP can be attacked through a cipher-text only attacked against the KSA of RC4. Some information about the individual key bytes can be leaked by the first byte generated by RC4 which means that if enough WEP-encrypted packets were analyzed, there could be possibility of reconstructing the key in WEP. Demonstration of this attack was later shown by Stubble-field et al.

The flaws in WEP can be summarised as follows:

- The forgery of packets cannot be prevented in WEP.
- Replay attacks are not prevented.
- RC4 was easily crack able.
- Weak keys could be cracked by brute force attack which only took minutes to hours on standard computers.
- The IV was being sent to receiver in the clear text which was not secure.
- CRC-32 checksum was weak and did not provide adequate security.
- 24-bits IV was relatively small which provided only limited initialization vectors, after that they were just being reused.
- The message can be modified without knowing the encryption key.
- Key management is not included.

Wi-Fi Protected Access (WPA)

WEP weakness is patched up to some extent through WPA. It implements Temporary Key integrity Protocol (TKIP), which allowed better mixing of the key with the IV. WPA was designed so that it could work with the existing hardware that was enabled with WEP. WPA included improvements that added more security features in the WEP.

The strengths of WPA can be summarised as follows

- It uses Temporal Key Integrity Protocol (TKIP) that is quick fix to the security problems of WEP without any requirement of hardware upgrade. Hashing algorithm is used to ensure the integrity of the key.
- The size of the IV is increased to 48 bits. It mixes the key well with the IV unlike in WEP.
- The sequence counter was used to prevent the replay attacks.
- Extensible Authentication Protocol (EAP) is used to provide a much stronger authentication.
- The integrity of the data is maintained through a Message Integrity Code (MIC) [9].

Vulnerabilities of WPA

In 2004, two tools were released to perform the brute-force attack on WPA-PSK to determine the passphrase. First tool was "WPA Cracker", it was released by Takehiro Takahashi and another tool known as "cowpatty" was released by Josh Wright [10], [6].

The flaws of WPA are as follows:

- WPA retains the old stream cipher RC4 which was already proved to be weak even in WEP.
- Brute force attacks are possible if weak passphrase
- Denial of Service attacks is possible in WPA .
- WPA has greater performance overhead unlike WEP.
- WPA-enterprise requires a complicated setup.

Wi-Fi Protected Access-2 (WPA2)

802.11i uses the Counter Mode with CBC-MAC Protocol (CCMP) and Advanced Encryption Standard (AES). CCMP along with AES provides WPA2 a stronger security as compared to WPA A stronger authentication is provided by 4-way handshake The comparison of all three protocols based on the common features has been shown in Table 1.

FURTHER DEVELOPMENTS

Hwang et al. proposed a wireless Man in the Middle (MITM) framework proving that a MITM attack is possible during the authentication mechanism if the attacker intrudes between the client and the AP. The procedure is shown in the Figure.

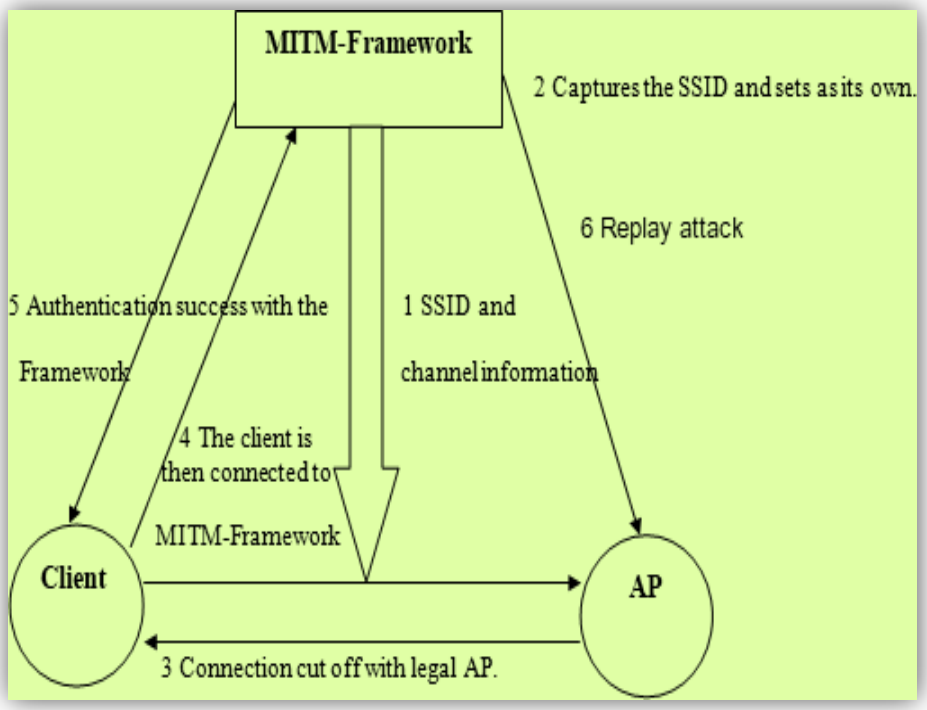

Figure7.2. Man in the Middle (MITM) framework

First the attacker captures the SSID and the channel information of the AP by listening to the communication between the client and the AP. The attacker then sets up the captured SSIS as his own and disconnects the client from the legal AP. When the client scans the network to reconnect through the MITM-Framework, it connects with the rogue AP of the attacker.

Even the 802.11w that was introduced to provide security to the management frames are vulnerable and can be exploited. The management frames can be forged in 802.11w and studies also shows that it is also vulnerable to Denial of Service attacks.. This standard was intended to prevent masquerading, detection of replay attack, forgery detection and prevention, despite all the added security features it still remains vulnerable. Some of these vulnerabilities are highlighted in Table 2 and the controls for some of these vulnerabilities are presented in Table 3. In the four-way handshake mechanism when the A Nonce is sent to the client by the AP, the client constructs the PTK+MIC. This construction process requires some time providing an opportunity to the intruder to send out malicious frames before the client replies with Snonce and MIC Also, no security is provided to prevent the attacker from eavesdropping the four-way handshake whatsoever. In another vulnerability related to four-way handshake the attacker can send fake authentication request after receiving third

message of four-way handshake process because after the client receives the Message 1 of the four- way handshake, a delay is caused by the generation of the PTKSA The amendment 802.11w does not mitigate this vulnerability because the attack takes places during the EAPOL four-way handshake.In 802.11w standard, CCMP from 802.11i is used to provide confidentiality, and the broadcast management frames are protected by the Broadcast Integrity Protocol (BIP). Protection is only provided for de-authentication and dissociation management frame subtype action

CONCLUSION AND FUTURE WORK

In this paper we presented the brief overview of the Wi-Fi security protocols: WEP, WPA and WPA2. Despite all the security features added to these protocols, they still remain vulnerable to certain attacks. The aim of this paper was to highlight the vulnerabilities and controls associated with these protocols. The paper briefly discussed about the vulnerabilities present in the 802.1X based Authentication mechanism of 802.11i. Finally, we presented some techniques to control these vulnerabilities propsed by various researchers.

REFERENCES

[1] Menal, “Evolution of Wireless LAN in Wireless Networks.” International Journal on Computer Science and Engineering (IJCSE), March 2017.

[2] S. Gopalakrishnan, "A survey of wireless network security." International Journal of Computer Science and Mobile Computing 3.1: 53-68, 2014.

[3] T. Mekhaznia, A. Zidani. "Wi-Fi Security Analysis." Procedia Computer Science 73: 172-178, 2015.

[4] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4" In Selected areas in cryptography, vol. 2259, pp. 1-24, 2001.

[5] A. Stubble, J. Ioannidis, A.D. Rubin, “A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)”, ACM Transactions on Information and System Security, Volume 7 Issue 2, pp. 319-332, May 2004.

Editorial Board

Editor-In-Chief *Prof. Mane S.S.*

Editor *Prof. Zaware G.B.*

Student Coordinators

- *Mr. Pawshekar Abhishek*
- *Ms. Gaikwad Pooja*
- *Ms. Randive Sonal*

Published By
Department of Computer Engineering
JSPM's
Bhivrabai Sawant Polytechnic, Wagholi,
Pune 412207,

www.jspmbspoly.edu.in *bsphodco@gmail.com*