THE SECURE AUTHENTICATION MECHANISM TO INCREASE SECURITY OF THE IOT DEVICES

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

GURJEET SINGH

Registration No. 11607216

Supervisor

HARWANT SINGH ARRI

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

Dec 2017

Dec 2017

INDIA'S LARGEST UNIVERSITY IN
LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE548 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0351

Supervisor Name : Harwant Singh Arri **UID :** 12975 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Gurjeet singh	11607216	2016	K1637	9041020499

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** _____

PROPOSED TOPIC : The secure authentication mechanism to increase security of the IOT.

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.80
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.20
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.80
5	Social Applicability: Project work intends to solve a practical problem.	6.80
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.20

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 3 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
PAC Member 4 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 5 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 6 Name: Aditya Khamparia	UID: 17862	Recommended (Y/N): Yes
PAC Member 7 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kuldeep Kumar Kushwaha	UID: 17118	Recommended (Y/N): Yes

Final Topic Approved by PAC: **The secure authentication mechanism to increase security of the IOT.**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal **Approval Date:** 04 Nov 2017

ABSTRACT

The Internet is a global system of interconnected computer networks that utilize the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of millions of private, public, academic, business, and government networks, from local to global in scope. the Internet of Things has turned into a leading path to the smart universe of ubiquitous computing and networking. It is depicted as a self-configuring wireless network of sensors whose intention is to interconnect all things. The secure channel establishment and mobility management are the two major issues of IOT which are highlighted in this research work. In the existing technique IPv6 proxy server is used which will provide end-to-end encryption and provide handoff in the network. The IPv6 provide handoff and also increase delay in the network at the time of data encryption. In this work, technique of ECC is proposed for the data encryption and angle of trajectory is applied for the soft handoff. The proposed improvement leads to increase network efficiency in terms of various parameters

DECLARATION

I hereby declare that the research work reported in the dissertation proposal entitled "**THE SECURE AUTHENTICATION MECHANISM TO INCREASE SECURITY OF THE IOT DEVICES**" in partial fulfillment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Harwant Singh Arri. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Gurjeet Singh

11607216

CERTIFICATE

This is to certify that **Gurjeet Singh** has completed **M.Tech** dissertation-II proposal titled "**The secure authentication mechanism to increase security of the IOT devices**" under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation-II proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engineering.

Date: 29/11/2017

Signature of Advisor

Name: Harwant Singh Arri

UID: 12975

ACKNOWLEDGEMENT

Though only my name appears on the cover of this dissertation, a great many people have contributed to its production. I owe my gratitude to all those people who have made this dissertation possible and because of whom my graduate experience has been one that I will cherish forever. My deepest gratitude is to my advisor, **Mr. Harwant Singh Arri**. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own and at the same time the guidance to recover when my steps faltered. He taught me how to question thoughts and express ideas. His patience and support helped me overcome many crisis situations and finish this dissertation.

Most importantly, none of this would have been possible without the love and patience of my family. My family has been a constant source of love, concern, support and strength, all these years. This accomplishment would not have been possible without them. Thank you.

Gurjeet Singh

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER-1

INTRODUCTION

With the advancement in mobile computing and wireless communications, a new paradigm known as the Internet of Things (IoT) is swiftly generating a lot of research interest and industrial revolution. The Internet of Things (IoT) could be described as the pervasive and global network, which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices.

1.1Internet of Things (IoT)

A global system that includes the numerous computer networks within it is known as Internet. In order to provide communication amongst innumerable users available, the standard Internet Protocol Suite (TCP/IP) is utilized. There are numerous types of users present within these networks which include private, public, government and such other sectors. With the advancement in technology over the years, in the 1970s the Advanced Research Projects Agency Network (ARPANET) was developed which continued till the 1990s. The network of interconnected regular objects is known as Internet of Things (IoT). Within various applications that include the various universities, the IoT has been utilized in order to provide computing and networking efficiently within them. The main objective here is to interconnect all the things present within this self-configuring wireless network which includes numerous sensors. An object that gets involved within a communication chain is also present. The combination of communication capabilities which are given by the data transmission is given by these lines present. RFID is known to be the main object within the IoT. The building of global infrastructure for RFID tags which is known to be a wireless layer present on the top of Internet. The communication is made amongst network of interconnected objects and the interconnected computers. There is a different Internet Protocol (IP) location for the objects at some instants. These objects are embedded within the complex systems. In order to gather the information here, the various sensors are used which gather information related to temperature, and other aspects present in the surroundings. The sensors present near to each other transfer the gathered

information in order to provide further processing as per the requirements of the current applications [1].

The IoT applications provide Internet and various advance software and communication services. Here, the objects can be connected to each other or to the things and can access the media present. The objects and things present worldwide can be interlinked with each other and provide access to communication in order to provide IoT environment. Being the part of small computer is the main criteria for each object or thing. Any kind of forecast present has been outperformed by the microchip to which the connection is made. The technologies present within the IoT are presented below:

• RFID

• Sensor and actuator

• Miniaturization

• Nanotechnology

• Smart entities

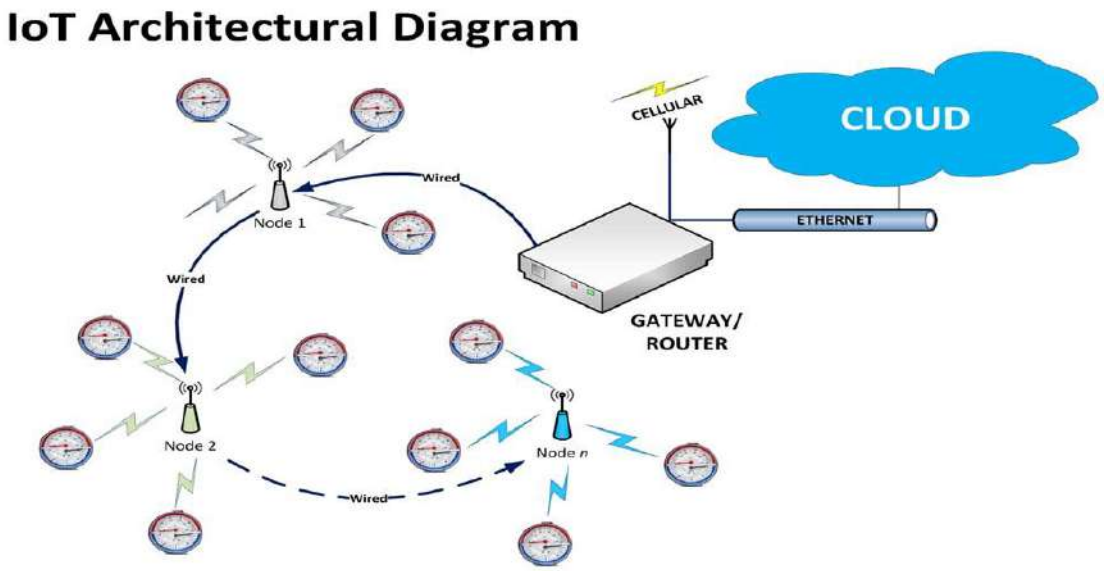

Fig 1: IOT Architectural

The substructure of IoT environment is the increment in the processing power that is present within the smallest packages or devices present within the network computing. Within the various technologies, the RFID and sensors are present which provide real-world environment within the IoT network devices. Within the real-time, object-to-object IoT applications are examined. This is done on the basis of the actual status along with the analysis of automatic reactions from IoT. In comparison to the objects or things that have no tags with unique visual or sensors, the method has resulted in providing smarter objects or things.

1.1.1 Characteristics of IoT [2]

- **Connectivity:** This feature allows in creating and processing the data traffic present within the IoT. The objects can be connected with each other either in wired or wireless manner. It is also allowed to establish the connection with the heterogeneous entities present within the IoT.
- **Connections:** There are entirely new dynamic networks generated with the multiplications in IoT. Within these systems, technological advances and visions of network ubiquity are used in order to develop the IoT systems and no fictions are included.
- **Embedding:** There are various gadgets and regular items in which the short-range versatile transceivers are present. This helps in providing new communication shapes for different users and things. This technology is further helpful for the objects as well present in IoT.

1.1.2 Service Search

Within the IoT applications there is a need to search the services which is done on the basis of some criteria. The object that needs to search the service first will search it amongst its friends or neighbors. The friends of the friends are approached in case the service required is not present amongst the friends of the objects. These results making this whole process a distributed searching process. One of the important search areas in IoT is the service searching method. In order to perform an operation or retrieve data that is present within some different device the searching of service process is accomplished. There are two categories in which the requirements needed for search are divided. They are point-based requirements and the proximity-based

requirements. The devices which search for particular objects use the point-based requirements however, the applications that include flexible search utilize the proximity-based requirement approach.

1.1.3 Applications and Things in IoT

There are numerous applications in which the IoT technology has been introduced which include the surveillance of forests, industrial automation, within transport services, smart homes and so on. The appropriate devices which are known as things are accessed by the system as per their applications within these applications. The numerous applications within these systems are explained in brief below [3]:

1) Smart Home: In order to facilitate the environment monitoring along with the control of electrical devices, the smart home applications are introduced. There is one control center present in this system which includes different types of electrical and agent devices within it. There are numerous functions included here which are the agent management, data transmission, access authentication and environment monitoring. In order to recognize the device and Bluetooth, the RFID technology is used. Further, the data is transmitted using the GSM modules. There are numerous electrical equipments included here along with the control function within the objects present in the system. With the help of all such home applications, the daily lives of people have improved and become easier. The automatic control functions have made it easier to access the management from far places as well.

2) Forestry Monitoring: This application includes the surveillance of forests and its surroundings. On the basis of Zig-Bee, the IoT forest environmental factors are designed. They are used for computing the environmental factors such as temperature, humidity and so on. In order to process, the gathered GPS and clock information is transmitted to the server. This helps in monitoring the forest resources in an effective manner. In order to gather all such information from the surroundings, the sensors are present within the objects of the systems. Further, the data is also transmitted with the help of wireless LAN within these systems.

3) Intelligent transportation: This application provides the facility of monitoring the conditions of traffic and provides data in order to manage the traffic and suggestions to the drivers as per their demands. There are fixed roadside detection units, on-board units present within the

vehicles, the backend server as well as the terminals for the client within this system. With the help of cameras placed on the roadside, the image is retrieved by the system. An end goal here is to determine the weather and the situations of the road. With the help of on-board units, the information of location of each vehicle is determined along with the speed with which it travels. The collected and aggregated data is sent to the backend server database with the help of 3G network. The users that have portable terminal are given the traffic data information gathered. The cameras help in attaining the information and the conditions of the traffic and weather surrounding them. The sensors placed within the environment help in gathering the information along with the 3G modules that are required for communication in these systems [4].

1.2 Properties of Things in IoT

There are various types of things which are different from each other with respect to the size and the various types. There are numerous features and access capabilities within the IoT applications. This, the properties or characteristics of IoT can be summarized into a few and are explained in brief as following:

A. Resource Granularity: Depending on the size of the things, they can be divided into two categories which are coarse and fine resources. On the basis of the complexity of the structure and its function, the granularity of the resources is determined. The basic structure and single function is present within the fine grain resources. The components of these resources include sensors, controllers, and RFID equipments within them depending on the type of resource in which they are being deployed. However, there is a complex structure and numerous functions present within the coarse gain resources. It also contains within it the fine grained resources along with numerous resources within it. There is a limited measure of fine-grain sensors present within a coarse-gain car for example. And, there are various functional fine-grain switches present within a coarse-grain household device. Further, there are various sub-divisions for it as well which depend on the type of device and the resource involved [5].

B. Functional Characteristics: There are two types of functions provided by the IoT, which are single function devices and complex function devices. There is only on type of basic function present within the single-function devices. For example, the environment prediction function is present within large number of sensors along with different controller devices within it. The

industrial as well as home applications can be handled with the help of these devices as they provide various sensors and controllers within them. In order to perform computing, the embedded processors are present within these devices. The data processing nodes and server nodes could utilize the data that is being processed here. The devices and objects that can perform numerous functions that have been represented earlier are known to be the complex function equipment. There are switch status perception functions and switch control functions for example, within a smart electrical switch.

C. Access Capabilities: There are equipment and resources present within the things used within IoT which can access the IoT as per the requirement. This can help in processing huge range of information that is required within these systems. In order to access IoT within a smart telephone or computer, only the hardware and software resources are not only the important necessities. IoT can be accessed by some industrial equipment which supports the M2M technology and other communication resources within these systems. There are numerous heterogeneous devices as well which are completely different from the listed categories. They have no resemblance with the existing real-world applications which are commonly known to the restricted devices as well. For example, the IoT cannot be directly accessed by huge range of sensors and sensor networks. This is due to the fact that there are very less number of resources present. Particular equipment needs to be handled here in order to provide potential access resources. The IoT is accessed here in inappropriate manner within these networks in order to provide proper communication amongst the objects [6].

1.3 Access Requirements of Things in IoT

There is a need to analyze the access requirements that are required within the access restricted devices of IoT. There are large numbers of access requirements present here which are not available in the real world with an extensive scale. There is lots of important data present within these things. The applications fields of IoT will expand more in case there are higher numbers of access restricted devices which have access to the IoT. This results in making the system more powerful as well as intelligent. There are functional as well as non-functional requirements which are present within the access restricted devices mostly. The categories are explained below:

A. Functional Requirements

There should a proper recognition of any access device present in IoT in initial stage. Further the operations are to be performed. The MAC or IP for example is utilized in order to recognize the computer when it has to access the internet. There is a need of external hardware and software resources in case when a particular task of computing function is to be executed within the access restricted devices. The control direction also for example is received with the help of the external communication modules by industrial controller in order to handle the intelligence. The analysis and summary of the access functional requirements is done on the basis of all such analysis and the following terms are stated:

1. Identification & authentication: With the help of specific recognition, the identification and authorization of things in IoT are to be done in a unique manner. The things can be operated and seen through in an independent manner with the help of this identification. There should be unique, traceable and controllable recognition within the IoT systems. There are numerous technologies also involved within this process which help in ensuring that the security methods are followed [7].

2. Environment perception: The surrounding information is perceived either by direct or indirect manner by the things. The compared information is processed further as per the applications in which the IoT is deployed. The communication interface is set up here by the access restricted devices within the environment. The interface communicated here with the special channels present between the perceptive terminal and service platform of the system. The various key techniques such as resource description and many other are present within this method.

3. Interactive control: In order to operate some particular equipment for automatic control and management, there are various objects present in IoT. The control channels are present amongst the control terminal as well as the service platform which are mainly required in order provide control channels within the access restricted devices. There are various techniques such as service publication and business function description which are part of this method.

4. Computing & processing: The computing and processing capabilities are available in some of the things present in IoT along with the environment perception and iterative control methods.

The computing and processing functions are to be identified within this type of access restricted device in IoT. Particular hardware and software resources are required for helping the data processing function and the business services [8].

B. Non-functional Requirements

The software and hardware resources here are mostly expanded in order to have performance requirements within the non-functional requirements. As per the hardware resources, there are some access devices that are restricted. In order to perform computations and for storage purposes there are some access restricted devices that are fixed. However, there are various other devices which cannot provide communication facility within them. There is a need for the access restricted devices to coordinate with a particular software and hardware in order to enhance the performance of hardware services and also to ensure better quality of service. This is however, difficult because the normal implementation of functions cannot be supported by the hardware performance of the IoT services [9].

There is an analysis and summary proposed n the basis of all such criteria for non-functional requirements which is provided below:

1. Unified access: The heterogeneity is to be prevented in case when the IoT is accessed by the access restricted devices. There is a need of providing the access requirements by keeping in mind the unified interfaces and protocols of the system. The data format and operation processes are also focused on within this process. This helps in providing this system a universal application development platform in order to provide better IoT interface. The general interface design is included within the unified access along with the adapter design and the multi-protocol implementation which can help in building efficient interface for IoT.

2. Platform expansion: The issues arising within the access restricted devices can be handled with the help of limited resources with the utilization of external resources and devices. The hardware and software platforms can be improved here as per these lines. The implementation of function is also to be handled within this process. The computing, storage and communication capabilities are also enhanced here. The resource consumption is minimized here along with making sure that the important functions are included [10].

1.4 Energy Harvesting in IoT

There are numerous applications included such as Internet-based vehicles, smart phones and so on, which are based on the IoT. However, there are simpler sensors and wireless devices present within the IoT network which also contain other things such as recognition of objects, control and sensing methods and so on. The highest volumes of all devices include the least complex inactive RF devices that have very short range. The cost of these devices is also very less there is higher functionality provided within the RF devices that have short range and are given more power. The mobile phones and personal computers that are linked with internet are not the only devices that use the IoT within them. There are other wireless connected as well which include innumerable things and objects which provide efficient utilization within them. There are innumerable batteries present within these things which need to be bought, maintained and disposed as per their lifetime and utilization. In order to recharge these remote devices by providing new energy, there is a need of energy harvesting mechanism. Amongst the numerous things and devices present in IoT, the wireless nodes that have sensors within them are one of these devices. The information related to the surroundings of the sensor nodes are gathered and passed to the network.

The placement of sensor nodes in different locations in order to gather all the surrounding information is the major requirement of IoT. However, a major issue arising here is the deployment of power-distribution wires which can be helpful in order to provide the life to batteries that are dead. The issue might not be of major concern if the number of batteries were less. However, due to innumerable number of batteries involved, this is of major issue. The cost of battery and the maintenance are both the important issues to be solved. In order to solve all such issues, the energy harvesting technique is used. There is various power generating components deployed within the systems as per these harvesting technologies. There is however, limited amount of energy harvested within these systems also. Thus, various enhancements are proposed with studies in order to enhance these systems [11].

CHAPTER-2

LITERATURE REVIEW

This research is based on the handoff and security issues in the IOT. In this chapter, the techniques are hand off which are proposed in the previous time is analyze in terms of description and outcomes

2.1. ANALYSIS OF LITRATURE SURVEY

Chinmaya Mahapatra et al., 2016 [12], proposed a wireless system which uses numerous protocols and devices in order to provide communication amongst the sensors and machines is known as Internet-of-Things (IoT). The real time sensors as well as the virtual online sensors are provided with various facilities such as collecting, storing, communication or processing the data within the IoT systems. It is thus important to handle the clients that require efficient energy and delivery of robust data. There is a huge system established in case when all the devices are virtually linked to each other and the connectivity within them is replaced by the other machines. This might as well result in presence of numerous protocols and standards within the system which might make it more complex and large is size. There is an association of the portable and battery operated systems with the IoT systems. Due to this there are innumerable users which are using this system these days which makes it difficult to handle such data and also to control the energy being consumed. The RFID tags based on Cluster Heads (CH) identification, data handling and energy harvesting are proposed in this paper. The energy efficiency and data delivery related problems occurring within the heterogeneous systems are handled by this method as per the results achieved. On the basis of methods of class, the simulation results show that the proposed method is enhanced and is better than the existing approaches. The energy consumption models are generated after each round as per the various gateways present within them. This results in improving the overall lifetime of the network.

George Smart et al., 2016 [13], discussed the introduction of energy harvesting within the IoT systems in order to provide uninterrupted operations within them is the main objective of future enhancements being made in this technology. A multi-transducer platform is generated in this paper for photovoltaic and piezoelectric energy harvesting in this paper. This platform helps in

collecting the raw material related to the harvested power which is mainly found within the internal as well as external systems. With the help of probability mixture models, the generated power profiles are linked with these methods. The present data and processing code are easily accessible in order to provide research within the various applications of IoT and WSN. The main objective here to present data-driven probability models to the IoT which can help in controlling the energy production. This will help in coupling the energy harvesting measurements along with the energy consumption models. They can provide the processing and transceiver designs so that the IoT can be deployed in better way in future. Various tests are performed on the basis of practical transducer technologies such that the deployment of IoTs can be better. As per the various experiments conducted, it is seen that the efficiency of IoT systems is enhanced in comparison to the existing approaches.

Xenofon Fafoutis et al., 2015 [14], discussed the designing and execution of MAC layer present within the wireless embedded systems is presented in this paper. The novel protocol features are presented in this paper with the help of power harvesting methods. There are numerous researchers who have generated their own practical solutions and have excluded the basic standards that are to be imposed. This study includes all such enhancements which can be useful in proposing future studies. On the basis of receiver-generated method of asynchronous methods, the ODMAC method is introduced in this paper. This is basically an energy-based MAC protocols that will help in reducing the issues arising due to energy harvesting. A sustainable performance is provided by the single control cycles that are generated due to the features of new protocols. This helps in enhancing the energy efficiency of the complete system. In order to provide enhancements within MCU, the ODMAC method is implemented. The hardware is utilized in order to conduct experiments on this method. As per the results achieved it can be seen that there are long-term sustainable operations performed which help in providing configuration parameters within the system. In order to communicate between the sustainable throughput and link-delay, the proposed method provides long-term sustainable operation. Further, it is seen that the energy efficiency of the link is enhanced within this method in comparison to the previous methods due to the presence of opportunistic forwarding and back off mechanisms.

Maria Gorlatova et al., 2015 [15], presented a paper, in order to improve the energy efficiency of the IoT systems, the kinetic energy is harvested. This is done with the help of wireless nodes present within these systems from which the energy allocation algorithms are developed further. A novel approach is proposed here which can generate energy from the acceleration activities. In order to determine the amount of energy that can be generated by human activities, 40 numbers of participants were involved in order to generate a motion dataset. The energy generation forms of human routines were gathered which recorded their movements for about 200 hours. The experiments conducted related to the mobility of items are presented in this paper. The energy allocation algorithms were generated which involved the practical node design. The gathered measurements were utilized in order to evaluate those algorithms. In order to design the motion energy harvesters and the respective algorithms, there is a need to outline the perceptions that are to be involved here. A wireless energy harvesting node model is presented in the proposed method that includes the practical design of nodes present within IoT. The performance of the proposed method is computed on the basis of gathered motion energy traces.

Xiaosen Liu et al., 2016 [16], discussed in order to provide energy harvester for the smart nodes within the IoT systems, the monolithic microwatt-level charge is used which pumps the extra required energy within these systems. The charge pump was optimized within the proposed architecture and circuit level researches due to the differences within the accessible voltage and power. The hybrid conversion ratios are provided in order to reduce the charge redistribution loss within a reconfigurable charge pump in the initial stage. With the help of frequency modulation, the reconfigurable feature is turned into maximum power point tracking (MPPT). This results in generating a 2D MPPT system. As a sensing approach, the MPPT method is used along with the constant-on-time (COT) scheme which is a regulation part. This helps in removing the method that provides energy within the latest technologies. The energy sources are harvested with the help of proposed method that includes large number of smart nodes in it as well. It is seen as per the simulation results that the proposed method resulted in providing simple and enhanced PCE method that provides very high power.

L. Roselli et al., 2015 [17], discussed in order to utilize the IoT is a realistic manner; there are various technologies that are mostly contributing which are to be studied in this paper. Along with the advancements made in IoT these technologies have been evolving. The various

technologies being introduced with time are Radio Frequency Identification (RFID), Green Electronics (GE), and many others which have been providing various advancements in the previous versions and provided reliable methods to provide better communications. All such methods are collectively presented here in order to be studied as experiments which are the major study of this paper. Within the related papers, there is a proper description related to the proposed methods. The image which is comprehensive and not much expensive is presented in this paper which is utilized as a part of this experiment. It is seen through the experimental results achieved that all these approaches have been playing important roles in handling various scenarios and the only thing that is to be focused on is their support with the major IoT guidelines.

Yiqun Wang et al., 2015 [18], proposed a switching-mode power converter (MPPT), charger is proposed in this paper which helps in managing the current that modifies to the energy storage element. This helps in providing power to the load device present in the system. With the help of energy storage element, the difference between the maximum power point (MPP) current and the load current is controlled. There is significant loss of energy and weight/volume within this system. Also the cost is exceeded mainly due to the cascaded power converters and elements of energy storage present within these systems. The MPPT is used with the converter-less PV system in this proposed method which will help in supplying power to the load. There are no power converters or energy storage elements present here. In order to take control over the fine-grain dynamic power management system, the non-volatile microchip is used in this method. The load current is matched here with the MPP current of the system. It is seen through the various conducted experiments that the efficiency of the complete system is enhanced along with the achievement of higher duty cycle.

Luca Roselli et al., 2014 [19], presented one of the most famous technologies that include RFID within it is mainly utilized in order to gather energy which is used in deploying the IoT systems. A wide class of systems is presented in this paper which comes user the category of large area electronics (LAE) which is a part of IoT and the smart surfaces are utilized in order to represent it. Initially, the review is presented related to the presence of IoT and LAE in this paper. Further, the architecture and techniques utilized within this method along with the usage of antennas, RFID and other devices is also presented in this paper. These devices are studied in order to

study the design and architecture of these systems. Further, the solutions are simplified which help in studying the development of relevant techniques within this area. This study might help in developing the other solutions which might be required in other studies. The experiments made help in determining the conclusions in this paper. This paper helped in providing solutions to the various issues that aroused within the techniques that included acceleration during the deployment of the IoT systems.

Pouya Kamalinejad et al., 2015 [20], proposed a system that includes simple physical objects which have unique identifiers and can be linked with the Internet in order to provide human communication is known as Internet of Things (IoT). The important components that are to be utilized within this acknowledgement are the long-term and self-sustainable operations. The energy related devices are included here that mainly gather the energy that is needed from the nearby related sources of these systems. A review is presented in this paper which is related to the enabling of technologies in order to provide efficient WEH. Further, the lifetime of the WEH-enables IoT systems is presented in this paper. The future work related to the design of efficient WEH systems and challenges is presented in this paper as well. The technologies and plans that are used to empower the WEH are also studied in this paper. In order to improve the efficiency of these systems and minimize the energy consumption of devices, there are studies proposed. For two different scenarios, the lifetime of the WEH is divided within the battery operated systems. There are various experiments conducted that include such scenario and it is seen that the energy efficiency is enhanced within the self-sustainable environments. However, there are numerous drawbacks seen within these scenarios as well as these systems are not applicable for all the different conditions. Thus the future work holds all such changes to be made within this proposed method so that this drawback can be eliminated. Numerous measures are taken such that the proposed method can help in removing all such issues that might affect the energy efficiency of this method and provides reliable conditions.

2.2. INFERENCES DRAWN FROM LITERATURE REVIEW

The Internet of things is the decentralized type of network in which sensor nodes sense the information and pass that information to the base station. The base station will publish sensed

information on internet. The security, handoff and energy consumption are the three major issues which are highlighted in the literature survey. :-

1. Due to decentralized nature of the network, the sensor nodes which sense required information may be the malicious which are responsible to trigger various types of security attacks which reduce network information. The researchers proposed various types of secure algorithms but yet not any algorithm is proposed which provides complete network security.

2. In the network, the sensors of end users may be mobile due to which mobility management; handoff mechanism is required which provide soft handoff in the network. The mobility management techniques need to be designed to increase network performance.

3. The sensor nodes which sense conditions are deployed on the far places and very small in size due to which energy consumption is the major issue of IoT. The energy of the network is consumed while transmitting and receiving data from any source. The energy consumption can also be addressed to increase network performance.

4. The Researchers has proposed various techniques to manage security issues and also to maintain soft handoff in the network. The security of the network get compromised when handoff get initiated. The technique is required which maintain network security at the time of handoff.

CHAPTER-3

PROBLEM DEFINITION AND PROPOSED WORK

In the previous chapter, various research gaps are highlighted on the basis of literature survey. The literature survey finding explained that security and mobility management are the major issues of IoT which needs to resolve to increase the network performance. In the past time, various authors provide solutions to these problems but completed and efficient framework is not yet proposed to resolve the mentioned problem.

3.1. Problem Definition

The idea of this research comes from the, "Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks", which is proposed in 2016 by Daemin Shin el al. The author highlights the issue of routing and secure channel establishment from source to destination. To establish secure path and handle mobility IPv6 Proxy is used which handles mobility and also provides secure channel between two parties. To provide end-to-end encryption and to implement soft handoff mechanism technique of elliptic curve cryptography and angle to trajectory is applied in the network. The major issues which are described in the paper is mentioned below:-

1. In the existing technique, the IPv6 is the proxy server which is implemented to provide end-to end encryption over the channel which is used to transmit data. The IPv6 is complex and increases network delay at the time of encryption and decryption.

2. The technique which is proposed in the existing system for the mobility management depends upon the IPv6 protocol. When IPv6 protocol is implemented for the mobility management it leads to hard handoff which reduces network performance. The soft handoff mechanism is required for the mobility management in the network.

3.2. Objectives of Proposed Work

1. To improve performance of Secure and Efficient Protocol for Route Optimization by applying end-to-end encryption and soft handoff in terms of Packet Drop, Delay and Energy Consumption.

2. To reduce delay in the data encryption and decryption by implementing elliptic curve cryptography for end-to-end encryption

3. To increase efficiency of the network for mobility management by implementing technique of angle of trajectory for soft handoff

4. To analyze the performance of proposed algorithm and compare with existing algorithm in terms of various parameters such as Packet Drop, Delay and Energy Consumption.

3.3. Research Methodology

The proposed work provides the solution to the problems which are mobility management and secure channel establishment from source to destination. In the past time various techniques are designed which provide solution to mobility management and security issue. This research is to improve handoff mechanism and increase security of the network.

1. Tool Description

The network simulator version 2 is the tool which is used to simulate the network modals. The NS2 is the event based simulator in which events are created and these events are triggered on the defined amount of time. The Ns2 provide both type of text based and animation based simulation. The animation based simulation is seen in the animation file called filed NAM. The second type of simulation is called trace file. The back end of the Ns2 is the C++ and front end is the TCL scripts. The results are analyzed in terms of graph.

2. Mobility Management Problem

The IoT network is the decentralized type of network in which sensors sense information and pass that information to the base station. The sensor nodes may be mobile which change its location any time, and due to which handoff can be implemented. In the existing technique IPv6

proxy is applied to handle mobility management which leads to hard handoff in the network. In the research, the technique of angle of trajectory will be applied which leads to soft handoff in the network

3. Secure Channel Establishment

The second major issue of the internet of things is the security. The IoT is the decentralized network and malicious nodes enter network which are responsible to trigger various type of active and passive attacks. The secure channel establishment is the technique which provides end-to-end encryption to the data which is transmitted over the secure channel. The IPv6 is the complex algorithm which provides end-to-end encryption. This research elliptic curve cryptography technique is implemented which is secure and less complex.

FLOWCHART

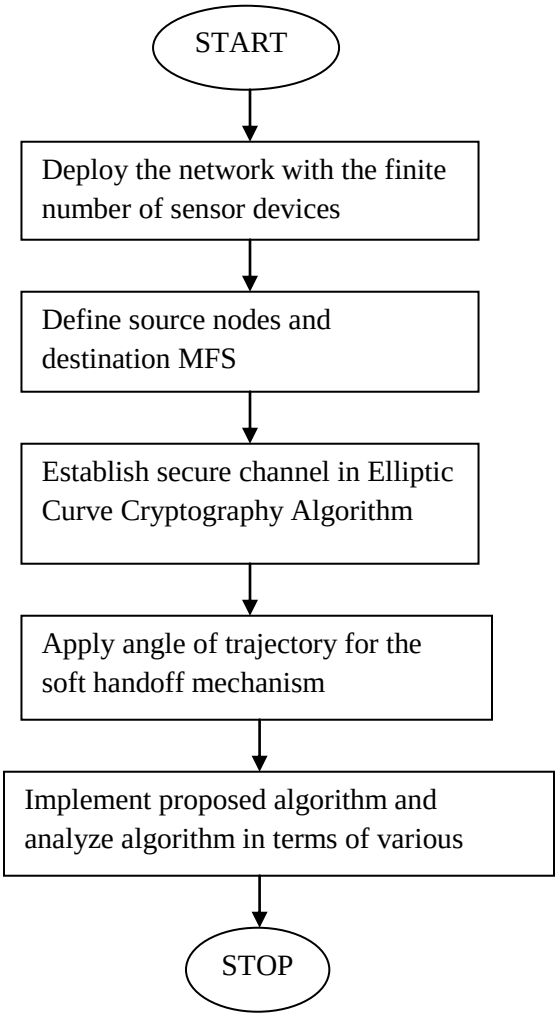

Fig 1: Proposed Flowchart

CHAPTER-4

EXPECTED OUTCOME OF PROPOSED WORK

Following are the various advantages of the proposed work:-

1. The proposed technique can increase security of the IOT network when the secure channel get established from source to destination.

2. The proposed technique leads to soft handoff in the network which can reduce network interruptions and increase network performance.

3. The complexity of the system is reduced for data encryption and decryption which reduce network delay.

4. The proposed technique can also increase efficiency of proposed algorithm with mobility management.

CHAPTER-5

CONCLUSION

The network of interconnected regular objects is known as Internet of Things (IoT). Within various applications that include the various universities, the IoT has been utilized in order to provide computing and networking efficiently within them. The main objective here is to interconnect all the things present within this self-configuring wireless network which includes numerous sensors. An object that gets involved within a communication chain is also present. The combination of communication capabilities which are given by the data transmission is given by these lines present. RFID is known to be the main object within the IoT. The building of global infrastructure for RFID tags which is known to be a wireless layer present on the top of Internet. This research work, is based on the handoff mechanism which can be triggered in IoT. The angle of trajectory technique will be applied which can do soft handoff in the IoT. The security technique will be applied in future which can improve privacy of the network

REFERENCES

[1] D.P.F. Moller, "Introduction to the Internet of Things," Springer International Publishing, volume 4, issue 17, pp- 239-246, 2016.

[2] Deepak Mishra and Swades De, "Energy Harvesting and Sustainable M2M Communication in 5G Mobile Technologies," Springer International Publishing Switzerland, volume 15, issue 22, pp- 12-25, 2016.

[3] Shulong Wang, Yibin Hou, Fang Gao1 and Xinrong Ji, "Access Features Analysis of Things in the Internet of Things," IEEE, volume 2, issue 9, pp- 423-431, 2016.

[4] Archudha Arjunasamy, Thangarajan Ramasamy, "A Proficient Heuristic for Selecting Friends in Social Internet of Things," ISCO, volume 11, issue 6, pp- 94-99, 2016.

[5] Minchul Shin, Inwhee Joe, "Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things," IET Commun., Vol. 10, Iss. 12, pp. 1508–1521, 2016.

[6] Kun Wang, Xin Qi, Lei Shu, Der-Jiunn Deng, and Joel J. P. C. Rodrigues, "Toward Trustworthy Crowdsourcing in the Social Internet of Things," IEEE, volume 10, issue 3, pp- 1536-1284, 2016.

[7] Dongsik Jo and Gerard Jounghyun Kim, "ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere," IEEE Transactions on Consumer Electronics, Vol. 62, No. 3, pp- 192-203, 2016.

[8] David Linthicum, "Responsive Data Architecture for the Internet of Things," IEEE, vol 5, issue 14, pp-117-129, 2016.

[9] Jun Qi, Po Yang, Martin Hanneghan, Dina Fan, Zhikun Deng, Feng Dong, "Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment," IET Netw., Vol. 5, Iss. 5, pp. 107–113, 2016.

[10] Haojun Huang, Jianguo Zhou, Wei Li, Juanbao Zhang, Xu Zhang, Guolin Hou, "Wearable indoor localisation approach in Internet of Things," IET Netw., volume 9, issue 8, pp. 1–5, 2016.

[11] Zhaoyang Zhang, Xianbin Wang, Yu Zhang, and Yan Chen, "Grant-Free Rateless Multiple Access: A Novel Massive Access Scheme for Internet of Things," IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 10, pp- 592-604, 2016.

[12] Chinmaya Mahapatra, Zhengguo Sheng and Victor C.M. Leung, "Energy-efficient and Distributed Data-aware Clustering Protocol for the Internet-of-Things," IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), volume 4, issue 33, pp- 643-651, 2016.

[13] George Smart, John Atkinson, John Mitchell, Miguel Rodrigues and Yiannis Andreopoulos, "Energy Harvesting for the Internet-of-Things: Measurements and Probability Models," IEEE, vol 3, issue 7, pp- 65-77, 2016.

[14] Xenofon Fafoutis, Alessio Di Mauro, Charalampos Orfanidis, and Nicola Dragoni, "Energy-Efficient Medium Access Control for Energy Harvesting Communications," IEEE Transactions on Consumer Electronics, Vol. 61, No. 4, pp- 173-180, 2015.

[15] Maria Gorlatova, John Sarik, Guy Grebla, Mina Cong, Ioannis Kymissis, Gil Zussman, "Movers and Shakers: Kinetic Energy Harvesting for the Internet of Things," IEEE, vol 6, issue 2, pp- 181-193, 2015.

[16] Xiaosen Liu, Lilly Huang, Krishnan Ravichandran, and Edgar Sánchez-Sinencio, "A Highly Efficient Reconfigurable Charge Pump Energy Harvester with Wide Harvesting Range and Two-Dimensional MPPT for Internet of Things", IEEE JOURNAL OF SOLID-STATE CIRCUITS, Volume 9, issue 3, pp- 552-562, 2016.

[17] L. Roselli, C. Mariotti, P. Mezzanotte, F. Alimenti, G. Orecchini, M. Virili, N.B. Carvalho, "Review of the present technologies concurrently contributing to the implementation of the Internet of Things (IoT) paradigm: RFID, Green Electronics, WPT and Energy Harvesting," IEEE, volume 19, issue 44, pp-622-639, 2015.

[18] Yiqun Wang, Yongpan Liu, Cong Wang, Zewei Li, Xiao Sheng, Hyung Gyu Lee, Naehyuck Chang, Huazhong Yang, "Storage-less and Converter-less Photovoltaic Energy Harvesting with Maximum Power Point Tracking for Internet of Things," IEEE, volume 14, issue 8, pp- 33-42, 2015.

[19] Luca Roselli, Nuno Borges Carvalho, Federico Alimenti, Paolo Mezzanotte, Giulia Orecchini, Marco Virili, Chiara Mariotti, Ricardo Gonc¸alves, and Pedro Pinho, "Smart Surfaces: Large Area Electronics Systems for Internet of Things Enabled by Energy Harvesting," IEEE, volume 16, issue 9, pp-507-519, 2014.

[20] Pouya Kamalinejad, Chinmaya Mahapatra, Zhengguo Sheng, Shahriar Mirabbasi, Victor C. M. Leung, and Yong Liang Guan, "Wireless Energy Harvesting for the Internet of Things," IEEE, vol 6, iss 16, pp- 77-83, 2015.