THE SECURE AND EFFICIENT DATA ROUTING TECHNIQUE FOR INTERNET OF THINGS.

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

By

Tanisha

11607148

Supervisor

Harjit Singh

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

November 2017

ABSTRACT

The IoT is the decentralized network in which the devices can sense information and upload that information to the server. The clocks of the IoT devices are not well synchronized due to which security of the network gets compromised. In this research work, the technique will be proposed which will synchronize clocks of the IoT devices and also establish secure channel from source to destination for data transmission. The proposed improvement leads to increase security of the network and reduce packetloss in the network.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation/dissertation proposal entitled " **THE SECURE AND EFFICIENT DATA ROUTING TECHNIQUE FOR INTERNET OF THINGS.**" in partial fulfilment 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. Harjit Singh Sir. 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.

TANISHA

11607148

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation/dissertation proposal entitled "**THE SECURE AND EFFICIENT DATA ROUTING TECHNIQUE FOR INTERNET OF THINGS."**, submitted by **Tanisha** at **Lovely Professional University, Phagwara, India** is a bonafide record of his / her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Harjit Singh

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

Gratitude cannot be seen or expressed. It can only be felt in heart and is beyond description. Often, words are inadequate to serve as a model of expression of one's feeling, specially the sense of indebtedness and gratitude to all those who help us in our duty. It is of immense pleasure and profound privilege to express our gratitude and indebtedness along with sincere thanks to our mentor **Mr. Harjit Sir**, for her invaluable guidance, motivation and encouragement in spite of her busy schedule.

I am grateful to our Lovely Professional University for me with an opportunity to undertake this research topic in this university and providing all the facilities.

Finally, we would like to thank our parents and our family members for their constant support. We whole heartedly thank them all for their encouragement and support all the way from home from their hearts. We dedicate all our success to each one of them.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO INTERNET OF THINGS (IOT)

A worldwide system that connects all the computer networks with the help of a standardized Internet Protocol Suite (TCP/IP) to provide various services to them is known as Internet. There are millions of users connected across the globe within the private or public sectors, business or government networks or within a local or a global range. The development of Internet has been since the 1970s and has grown around 1980s. However, its usage has mainly grown worldwide within the 1990s. The network interconnection of the regular objects is known as IoT. As there has been an increase in growth of the speed of computations and networking, the IoT has led to a path of smart universe. IoT is a self-configuring type of network which mainly interconnects all the things or objects present within the wireless network. Any item present within the real world that provides communication chain within the regions is known as an entity or object. The communication possibilities that can help in providing data transmission within certain paths with the help of various objects are the main goal of the IoT systems. RFID (Radio Frequency Identification) is the main goal of the IoT systems. A global infrastructure can be built for RFID tags within the IoT which can mainly be performed with the help of a wireless layer present on the top of the Internet providing the services [1].

The presence of Internet advances in software and telecommunication services which further help in connecting the objects with other potentially capable objects for providing the accomplishment of various services is provided within the IoT. The idea or service to be provided can be of a small computer along with a microchip present in it for providing a forecast of certain area. This is done with the help of joint work of various objects as shown in Fig. 1.1. The various technologies that are involved within the IoT are:

• RFID

• Sensor and actuator

• Miniaturization

• Nanotechnology

• Smart entities

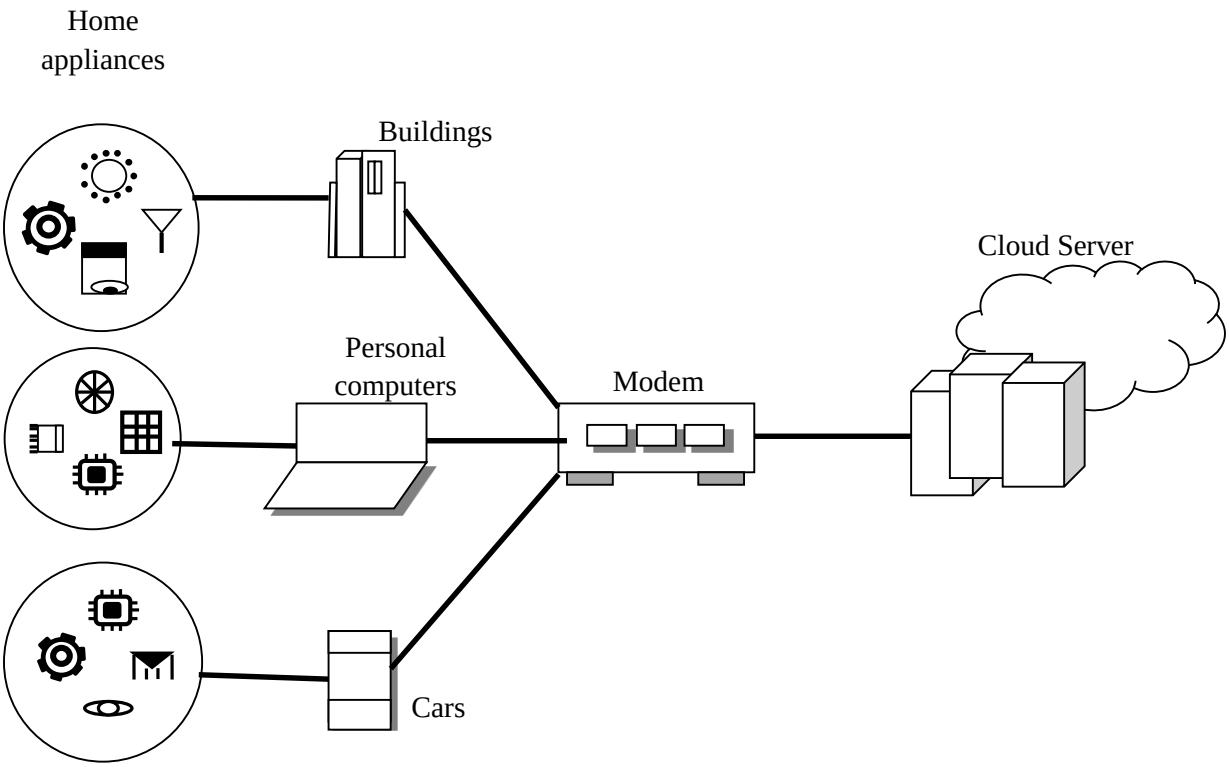

Fig. 1.1: IoT architecture

1.1.1 APPLICATIONS OF IOT

There are many applications promised by Internet of Things which can make life of humans easier, smarter and safer [3]. Few very important applications of IoT can be explained as smart cities, homes, smart environment and energy and smart health. Few of these are explained as below:

1. Smart Cities: Smart projects have supported many major cities like New York, Dubai and Singapore. It can be still considered as a future thing when we talk about smart cities with smart projects. IoT can really play a very important role in making the cities smarter and helping them in their development process in a simple and environmental friendly way [23]. Careful planning in every stage plays a very important role in the development of smart cities. The agreements with government have to be taken in a strict care while implementing IoT in the concept of smart cities. Improvement of infrastructure, making public transport better, reducing traffic jams and taking care of the safety of people are few

very important things to be considered [26]. Smart cities also include proper healthcare facilities, weather monitoring equipment and internet services in all the areas of the city.

2. Smart Homes and Smart Buildings: When we talk about smart homes, one thing which comes in our mind as the very first thing in wi-fi connectivity. A smart home is a home in which electronic devices such as mobiles, tablets, television; laptops are connected with the wi-fi. Wi-fi's have become a very important aspect of smart homes systems because they allow us to get connected with whole outside world while sitting at our homes. With the use of the concept of Internet of things, homes and buildings can operate many electronic devices and objects smartly [22]. Few IoT applications at smart homes can be considered as smart lighting, smart air conditioning, smart room heating and security.

3. Smart Energy and Grid: A grid which is controlled by the integration of information and communication technologies can be surely considered as a smart grid. With the use of such kind of technology there can be a two way real tie communication between the suppliers and consumers which will make the energy flow more volatile and dynamic. Sensing technologies, Digital communications are few key elements of use of internet of things technology in smart energy and grid. Few other applications like solar power, nuclear power and hospital power controls can be handled with the use of internet f things technology.

4. Smart Health: IoT can play a vital role in monitoring the health status of the patients who are admitted in the hospital because of any disease or physical issue. Smart sensors can be used to gather various information's about the patient's health status which can be further used to diagnose and treat the disease. The use of such sensors replaces the process of physical checkup by a doctor by visiting the patient of very small intervals [28]. It also plays an important role in the improvement of the quality of care and also reduces the cost of treatments.

1.1.2 FEATURES OF IoT

Here are few features of internet of things technology as defined as:

1. Interconnectivity: IoT provides a favorable and intelligent platform for connecting anything and everything with information and communication infrastructure.

2. Things-related Services: If someone wants to provide things related services for staying within the constraints then IoT can provide a very good platform for that, as IoT can create privacy protection between physical things and their associated virtual things.

3. Heterogeneity: IoT devices can easily interact with other devices and technologies with a straight forward use of Networks. Since IoT devices are based on different hardware platforms so they can also be called as heterogeneous devices

4. Enormous Scale: Efficient data handling is very important no matter if the number of devices that need to be managed are larger in number as compared to the number of devices currently connected to Internet. With the IoT we can do efficient data handling in critical conditions [27].

1.2 KEY CHALLENGES OF IoT

There are few challenges which arise while working with IoT technology. We have listed few of them below:

1. Heterogeneous Things: As IoT technology runs on different heterogeneous gadgets so the biggest challenge which arises while the use of these gadgets is to develop a communication among these devices which is supported by all of the devices. Since these devices are diverse in terms of correspondence [31], information storage ability and accumulation, so communication between them is always a challenging task.

2. Energy: Since the devices which form the base of IoT are deployed at remote places and are wireless appliances, so energy becomes a dominant issue in such cases. We have to make sure that we should develop such highly efficient algorithms and hardware which do not let the energy or battery drain quickly so that the sensor nodes can live for a comparatively longer duration.

3. Security: Just like any other technology, security is always a main concern for IoT. The security of data is the most important concern, so we need to use specific data isolation techniques to provide proper encryption so that the data reaches to the end user without any security breach. We also have to be careful that the algorithms we use should be energy efficient and can be used in very low power also.

4. Privacy: Violation of privacy is also one of the most important concerns while using IoT technology. There should be a proper algorithm to decide whether an access can be granted or denied to a particular data access request.

5. Intelligence: Improvement in machine automation can decrease the delay and traffic because this M2M (machine to machine) communication gets a very high priority in IoT. Smart technologies are needed to be more enhanced and updated to enable automated systems.

6. Clock Synchronization: It will be really tough to implement the 'Anytime' concept of IoT in reality. The real-time systems need to be implemented in grass root level of the IoT things to react prominently at any time. The clock synchronization is the real problem because of which it becomes difficult to implement IoT in the real time system. The efficient communication in the network is done when devices are properly synchronized which ensures end to end delivery of data without any delay in the network [23].

1.3 CLOCK SYNCHRONIZATION

Below are the explanations of the problems due to inaccurate clock synchronization and how those issues can be removed:

1.3.1 PROBLEMS DUE TO INACCURATE CLOCK SYNCHRONIZATION

1. Network Forensics: NAT (Network Address Translation) is used by all telecom operators because of lack of public Ipv4 addresses. By the use of NAT, one single IP (Internet Protocol) address can be used for multiple connections. To identify subscribers using the same IP at different times, it is utmost important to keep proper and accurate log of time. The log of time is generally maintained by the time set on the servers but this time is not always consistent [29]. Because of this issue of variation of time the service providers are unable to detect an exact subscriber which comes out to be a huge challenge in the use of IoT technology.

2. Reliability of time dependent services: The services which are completely dependent upon time accuracy are very much impacted by inaccuracy of time. For example in VoIP (Voice over Internet Protocol) services, for IP telephony reliability, accurate server and router log files are very important. Because of inaccuracy of time the working model of VoIP services is hampered [19]**.**

1.3.2 VARIOUS METHODS TO ATTAIN CLOCK SYNCHRONIZATION IN IoT

Below are few methods which can be used to get accurate clock synchronization.

1. Network Time Protocol (NTP): In NTP with the use of GPS (global positioning system) a proper synchronized time can be attained. The biggest advantages of using NTP system are that it provides high level accuracy and reliability in terms of clock synchronization [33].

2. Precision Time Control (PTP): PTP is a protocol which is used to synchronize a clock throughout a computer network. On a local area network it can achieve time and clock accuracy in sub-microsecond range which makes it a good match for measurement and control systems. It is basically designed for applications which cannot afford a GPS tracker at each node [31].

1.4 NEED FOR SECURE CHANNEL ACCESS

The secure channel establishment is technique which establish secure channel from source to destination. To maintain secure channel from source to destination the shared key is formed which will encrypt and decrypt data travelling on the channel with the same key.

1.4.1 WHY SECURE CHANNEL NEEDED?

1. Mutual Entity Authentication: To avoid any kind of impersonation by a malicious entity, all nodes in a network must be able to authenticate with each other in a proper manner.

2. Asymmetric Architecture: There should be a proper exchange of certified public keys between different entities.

3. Mutual Key Agreement: There should be an agreement between the communicating parties on the generation of a key during execution of protocol.

4. Joint Key Control: One party must be avoided from choosing a weak key by all communicating parties with a mutual control.

5. Key Freshness: To avoid replay attacks, the freshness of the newly generated key is very important.

6. Mutual Key Confirmation: there should be a confirmation by the communicating parties about generation of the same key.

7. Known-Key Security: If a malicious user obtains a session key, he/she must not be able to access long term secrets.

8. Perfect Forward Secrecy: If there occurs any compromise, this should not enable malicious user to compromise previously generated session keys [24].

1.4.2 TECHNIQUE USED TO MAINTAIN SECURE CHANNEL ACCESS IN IoT

1. Diffie-Hellman Algorithm for Security Access Protocol:

In the security access protocol, the two types of communication are possible between the gateways and the mobile devices. The data from the mobile devices is transmitted to the gateway which is transmitted to the IP-based backbone. The IP-based backbone will transmit data to service platforms. The Diffie-Hellman algorithm is applied to establish secure channel between the mobile devices and gateways for the bidirectional communication. In the communication, mobile device will select one public key and also select private key which is permitted root of public key. The gateway will also select one public key and also make private key which is primitive root of public key. The secure channel is established between the both parties when they agreed on the common key “k”. The data from the mobile device will be transmitted to the gateway through the established secure channel.

CHAPTER 2

LITERATURE REVIEW

C. Mahapatra *et al.* [1] stated that the systems that enable the various actions to be performed on the real time sensors as well as virtual online sensors are known as the IoT system. These systems help in sensing, collecting, storing, processing and transmitting the required data from the sensors. The main aspects here are the energy efficiency as well as the robust data delivery within these systems. In [1], the active RFID tags that were based on cluster head determination as well as energy harvesting of the IoT systems are proposed. As per the results it is seen that the IoT based WSN heterogeneous systems provide enhancement in the case of energy efficiency and data delivery. There is a great improvement seen through the simulation results achieved here. The energy consumption models have been formulated here as per the sensor nodes that were sent to the base station by the gateway nodes. The simulation depicted considerable improvement in lifetime of network and data delivery to the base station.

J. Yun *et al.* [2] presented a oneM2M standards-compliant device software platform for consumer electronics in light of the Internet of Things, called &Cube. It leverages a standardized resource model and REST (Representational State Transfer) APIs (Application Programming Interface) to work with oneM2M service platforms, prompting to interoperability crosswise over various IoT consumer electronics built on the &Cube [2]. The developing adoption of the &Cube in consumer electronics would lower the barriers for the manufacturers and developers to create innovative products and altogether new services.

L. Atzori *et al.* [3] provided an integration of various technologies and communication solutions within the Internet of Things. There are various components that together build in the deployment of Internet of Things. There are wired, remote sensor and actuator networks present within such systems along with the improved communication protocols. There are various activities performed by the IoT systems which can be monitored as per the needs. The activities performed can result in providing advancement in the IoTs and help perform learning mechanisms within them. There were applications that required a complex scenario to be established, which could be done with the help of performing various tasks within it that could support the complex nature and help in enhancing its

development as compared to the previous one [3]. The achieved results showed the enhancements made.

O. Novo *et al.* [4] proposed that the potential of this era is boundless, getting new communication opportunities in which ubiquitous devices blend seamlessly with the environment and embrace each aspect of our lives. The development of IoT has been proposed by the capillary networks which further helped in providing local remote sensor network for connecting and efficiently utilizing the capabilities of the gateways present within them [4]. As a result, a vast range of constrained devices equipped with just short-range radio could use the cellular network capabilities to increase global connectivity, supported with the security, management and virtualization services of the cellular network. The authors also introduced another Capillary Network Platform and depicted the rich set of functionalities that enabled this platform. To demonstrate their practical value, the functionalities were connected to a set of typical situations. The aim of their research was to give the reader insight about the Capillary Network Platform and illustrate how this work could be utilized to enhance existing IoT networks and tackle their problems.

J. Gubbi *et al.* [5] realized that on the basis of the growing remote technologies such as RFID tags, embedded sensor and actuator nodes there was need to enhance the IoT systems. The enhancements made so far have converted the Internet into a completely incorporated future Internet. The Internet services provided were on a very large scale and the enhancements to be made were to be performed in a very careful manner [5]. There was an increase in the need of data-on-request with the help of sophisticated queries being made when the data moved from www to web2 and further to web3. For the complete implementation of IoT systems, a Cloud driven version has been presented in this research which provides the necessities. The future technologies and application domains that are going to enhance the research work related to IoT are proposed. It is concluded by the experiments being conducted that the IoT systems viewed the expansion of their needs on the basis of various requirements within the networks.

H. Suo *et al.* [6] the author presented the security architecture and features of the IoT applications and provided the enhancements in the architecture. The challenges or vulnerabilities of the system are stated here along with the measures required to remove them. Various encryption mechanisms are proposed along with the communication security measures and cryptographic algorithms that could help in avoiding the loss of privacy of

the systems. The studies being proposed in the research has provided various guidelines to ensure the privacy and security of the IoT devices such that there could be no issues faced in the future [6]. However, even with the advancements made, there are lots of challenges being faced. The four layers present within the IoT systems are perceptual layer, network layer, support layer and the application layer. In this research the problems or attacks possible in all four layers are studied along with their characteristics and requirements. There is a need for various encryption mechanisms, protection for sensor data and encryption algorithms. The challenges being faced here are removed with the help of various measures and the results achieved are better as compared to the earlier mechanisms.

J. Granjal *et al.* [7] proposed that the architecture of IoT devices has IP-based communication protocols that provide the connectivity of devices as per the required applications. It was realized that there was a need of presence of such communication technologies in the areas where information sensing was very important. Keeping in context the goals of ensuring efficiency, reliability and internet connectivity, the various applications of IoT systems are proposed [7]. The communications being held within these systems was ensured to be protected which might only provide the usage of such applications more frequent. If the privacy or security was not assured, the users might not opt for their usage. The existing protocols as well as mechanisms that are required to secure the communications being held within IoT were broken down and completely studied. There are various challenges recognized within various IoT applications that are required to be removed from the system and thus, enhancements in the future are also stated in this research.

There is a presence of both IP as well as non-IP devices within the networks present in smart city services [8]. In the case of non-IP devices, the short-range connections were handled with a mediator gateway. This gateway helps in providing a capillary access network which is a short range extension of the traditional access network. The main objective is to capture the mobility of the IoT devices. On the basis of the terminal capabilities, the security algorithms are proposed by R. Giuliano *et al.* [8] for both uni and bi-directional terminals. On the basis of local key renewal based on the local clock time, the security algorithms are generated. There are two major factors that could help in affecting the performance of the systems. They are one mediator gateway and the maximum packet delay required as a function of the number of terminals present within the specific

area. As per the simulation a result, the performance improvement is assured and the changes made have proved to be beneficial.

S. Sicari *et al.* [9] proposed that there is a need of providing solutions to the IoT systems in such a manner that they are independent of the platform present within them and can provide confidentiality, access control as well as privacy irrespective of the platforms present. There was a need to provide various measures for building up the trust of the users to establish a communication within each other. This could only be done with the assurance of security by the two systems involved [9]. Due to the variety of levels and communication protocols involved, the earlier utilized countermeasures could not be implemented anymore. Also, when the number of users interconnected were more the complexity of the systems aroused within such dynamic environment. There is a need to identify the challenges being faced here and these challenges are resolved by proposing new methods that could remove such problems and provide a secure communication.

There are various data-communication tools required for providing the architectural design of the IoT systems. Mainly the RFID-tagged objects are involved within this task. The main objective of **R. Weber *et al.* [10]** is to ensure the exchange of objects within two systems along with the assurance of their security and reliability. There was a need to measure the resistance the system could provide to certain attack along with the authentication of data, access control as well as the privacy of the user [10]. There was need of the hidden technology along with the establishment of international legislator. This is provided by the private sector mainly according to the specific requirements of the user. The adjustments as per the needs of the user are ensured. There is a need to ensure that the right to information was successfully implemented within the systems and no restrictions are made on them for communicating amongst each other. Along with this, the principles required for maintaining the security are to be imposed within the systems. As per the results it is seen that the proposed changes has made the system more authenticated and helped in providing communication across the users without any privacy issues.

P. Wortman *et al.* [11] stated that the IoT devices are widely being used in the medical and healthcare domains. Coupled with the growth of information passed through these embedded systems, there was a clear and potential danger in having these IoT devices and networks not be held to indistinguishable rigorous standards of design from other industrial-level technology. In this research the issue of poor security designs and

implementation in medical IoT devices was addressed by proposing the utilization of existing modeling software AADL (Architecture and Design Language) as a method of institutionalization of medical IoT device development [11]. Generally speaking, the method would eventually need to measure the performance of these large IoT networks, however it is find that the result is totally different without some planning from a development stance. Consequently this work proposed utilizing the powerful and flexible modeling language AADL to account for constraints and different concerns of over-engineering IoT devices inside the healthcare domain.

Z. Guo *et al.* [12] proposed that the communication between the end points of devices with the help of physical objects present over the internet known as Internet of Things. The IoT services have known to provide ease in our day to day lives. But the systems have various vulnerabilities as well which might result in causing various issues related to the systems. There is a need of proposed examination of the systems from the very small level present within them. There is a need of proper communication amongst the devices and humans in case of IoT systems for their proper usage. So, the biometrics provided a proper mechanism for convenience and security within the IoT applications [12]. The merits and demerits related to the biometric within the IoT systems are also described. There are various issues such as reverse engineering, tampering and unauthorized access within the IoT systems that are to be prevented with the help of various new biometrics merged within the previous ones. It is seen through the results achieved that the enhancement made has been beneficial.

IETF impressively defined Internet interoperation crosswise over 30 years of unforeseeable punctuation API. IoT needs comparative future confirmation, however for associated things' composable semantics, security, reliability and QoS (Quality of Service). **T.Abels *et al.* [13]** review these with streamlining tradeoffs from a bottom up approach utilizing DDS (Data Distribution Service). At that point abnormal state semantic augmentations to DDS are suggested for semantics that were backward compatible, while keeping up the security, reliability and QoS of DDS. At last, additionally work is suggested toward out-of-the-box compos ability and interoperability between normal IoT information models and compliant arrangements. This author presents a SSN (Social Security Number) framework that consolidates the semantic endpoints of information centric with strong semantics, supporting resource discovery for semantic sensor and event annotations [13]. This initiates

composable semantics, while extensions remained DDS compatible for proceeding with information security, QoS and reliability.

M.Mohsin *et al.* [14] proposed an ontology-based framework for the IoT for providing security to these systems. There are various APTs (Advanced Persistent Threats) that occur within the systems and can be prevented with the help of certain measures. There are specific tasks that were performed here. The attack kill-chain is comprehended along with the leveraging of various attack examples and vulnerabilities. Further the network semantics are aligned for providing appropriateness within the IoT systems [14]. There are various already existing ontologies within the CTI (Cyber Threat Intelligence) standards which needed to be examined here. The comparisons of these already stated mechanisms are done with the new concepts and the novel IoT ontology is proposed. From the XML-based threat feeds, the related information is extracted by the framework. The simulation results achieved here showed the improvements that have been mainly seen with the help of new changes made.

There were various remote interfacing and monitoring issues that aroused when a device was connected with the Internet in the case of IoT. For the purpose of making an application smarter, safer and automated there was a need to enhance the working of such applications. A smart wireless home security system is highlighted in **R. Kodali *et al.* [15]** that sent alerts to the controller when any trespasser was seen within the system. This is done with the help of Internet. The alarm is raised in an optional manner and the concerned systems are notified regarding this issue. This method could similarly be applied in the home automation systems with the help of various sets of sensors in the systems which notified the important things and helped the actions to be controlled as per required [15]. As per the experimental results it could be seen that various enhancements when made within the systems, the applications could be made to run as per the needs of the users. Such enhancements are very useful and could be utilized in a huge number of applications mainly within the home automation systems.

The SBC (Smart Business Center) system was one of the most important subsystems within the IoT systems related to their security when the complexity was higher. The various issues arising in the design and operation of SBC systems are discussed in **V. Kharchenko *et al.* [16]**. The reliability and security of the system at various instants is to be done by examining their safety. The various levels such as the communication level, server level, and the

complete level of SBC subsystem is to be determined by these mechanisms. The SBC is designed in such a manner that the hardware and software mechanisms are seen by the manufacturers in a proper manner [16]. It is also important to ensure the security of SBC routers which could be done with the help of introducing various measures in it. The vulnerabilities detected within the system had resulted in exposing the system to hacker attacks which could destroy the privacy of the complete system.

The earlier researches proposed works related to the IoT systems have shown that these systems were vulnerable in a lot of scenarios. Each of the devices has various aspects of its own and is not similar to others. Hence, the security and privacy of that device was very difficult to be maintained. Various experiments were to be performed in order to provide the real aspects required for providing security within such applications. In A. **Tekeoglu *et al.* [17]**, a testbed is proposed for examining the security and privacy of IoT devices. Here, layer 2 and layer 3 packets are captured within this testbed. The packets that have various features were to be investigated within this paper. The cost of this proposed method is low as compared to other systems. It is based on off-the-shelf hardware and open source software. The security and privacy related issues within the various IoT devices are investigated here in a proper manner. The cameras, trackers smart watches and many other devices are utilized here for capturing the necessary information [17]. Various vulnerability related scans, identification of insecure protocol versions, firmware updates, and various other issues related to authentication and privacy are performed within the testbed. It is seen through the experimental results achieved that the proposed system provided better performance as compared to the other methods. The security and privacy of most of the applications that involved IoT devices could be done with the help of this method.

R. Giuliano *et al.* [18] in this paper, the main aim is to focus on the security of the aspects of IoT capillary networks. There are both unidirectional as well as bidirectional IP and non-IP devices present within the network. These all are present within the capillary networks and needed a secure access within them [18]. A local clock time and a time interval of key validity is to be ensured by the security procedure provided within the network. The duration of the validity of the time window is assessed within this paper. The simulation results are examined in terms of the time required for transmission within the realistic scenario along with the indication for setting time limit for the validity of the window. At

the end, the benchmark analysis is provided for assessing the effectiveness of the proposed method in terms of security when various attacks were present in the scenario.

I. Nasr *et al.* [19] proposed a clock synchronization algorithm which is based on the non coherent timing detection. The coherent timing detectors work on the Rayleigh fading channel technique for the clock synchronization in the IoT. The Rayleigh fading channel technique is very light weight due to which complexity of the system reduced to greater extent. The performance of the proposed technique was analyzed in terms of MSE (mean square errors) and it had been analyzed that it performs batter than NDA (Non Data Aided) Coherent technique for clock synchronization.

G. Giorgi *et al.* [20] proposed a clock synchronization technique for the Internet of things. It is been analyzed that IoT is the highly dynamic network to which time synchronization is the major problem in the network. The optimal solution to this type of problem is to reconfigure the devices for serving different applications. The proposed algorithm for clock synchronization is based on the re-configuring devices based on the references clocks. In the proposed technique three modules are used which are application interface, time reference unit and synchronization unit. The application unit maintains communication between low level and high level modules. The time reference unit gains the access of the local clocks and synchronization unit will adjust the clocks of the device according to application. The performance of proposed algorithm was tested in terms of accuracy in comparison to existing techniques.

K. Navneet *et al.* [35] stated that there is a need to minimize the energy used in the network and improvement in the synchronization of the sensors nodes. Due to the weak synchronization of the sensor network clocks, packet loss may occur within the network. This further might result in minimizing the lifetime of the network. This leads the need to enhance the working of the TDMA protocol as TDMA protocol is used to assign the time to various sensor nodes for efficient working of sensor nodes. In this paper, authors use NS2 simulation tool which involve the presence of finite number of sensor nodes and LEACH protocol is used for executing clustering and choosing cluster heads. In this paper authors proposed a time lay technique so that Radio Frequency Identification protocol can be improved and sensor nodes can be synchronized with the help of base station. As per the simulation results achieved it can be seen that the proposed algorithm performs well in terms of various parameters.

CHAPTER 3

SCOPE OF STUDY

3.1 PROBLEM DEFINITION

In order to improve security in IoT, there is a need to come up with a solution which will provide efficient communication between IoT devices. R. Giuliano et al. [18] has discussed the technique Diffie-Hellman, which is based on to generate symmetric key for secure channel generation between source and destination. For the purpose of encryption and decryption of data, the symmetric encryption algorithm is used and key which is used for encryption and decryption is renewed time to time. To maintain time synchronization between source and destination, NTP is used; the NTP protocol uses GPS for clock synchronization which consumes network bandwidth and hence increases bandwidth consumption of the network.

So, to provide enhanced clock synchronization and secure channel access for both unidirectional and bidirectional communication, we have come up with a solution where we will use RSA algorithm to establish secure channel from source to destination. This will lead to increased security of the network. For efficient clock synchronization, technique of time lay will be designed for IoT devices. The WSN is the decentralized network in which no central controller is present and sensor nodes keep on joining the network any time. The whole network is divided into fixed sized clusters and in each cluster, cluster head is selected on the basis of distance and energy. The cluster head takes initiative to synchronize the clocks of the sensor nodes which are in their cluster. When the clocks of all the sensor nodes which are in the cluster get synchronized, then cluster heads will communicate which each other to synchronize their clocks. The architecture of IoT network is different from wireless sensor networks due to which the gateways take initial step for the clock synchronization. The gateway passes the clock synchronization message to the IoT devices. The IoT devices will communicate with each other to synchronize their clocks and after that gateway node will synchronize their own clock.

CHAPTER 4

OBJECTIVES

This research work is done with the objectives mentioned as:

1. To study and analyze various security algorithms for secure channel access in IoT.
2. To implement the RSA algorithm for secure data communication in the IoT network.
3. To implement time lay technique for efficient clock synchronization of nodes in the IoT network.
4. To analyze the performance of both the NTP based and time lay technique for clock synchronization.
5. To compare results in terms of energy, throughput and packet loss.

CHAPTER 5

RESEARCH METHODOLOGY

This work is based on clock synchronization and secure channel establishment for communication in IoT. To introduce the clock synchronization, the technique of time lay will be used in which base station of each cluster of nodes will share its clock time with internal nodes of its own cluster, they in return share their clock time with base station. Base station will then calculate the average clock time. Similarly the other clusters of that network calculate their average clock time. After this all clusters will share their calculated clock times with each other and finally the clock of all clusters is set according to this new calculated average. In this way it will provide efficient clock synchronization. The secure channel establishment technique will be applied for both uni-directional and bi-directional communication. The technique of RSA algorithm will be applied which establish secure channel from source to destination. This leads to increased security of the network. Also, asymmetric keys will be exchanged through the secure channel.

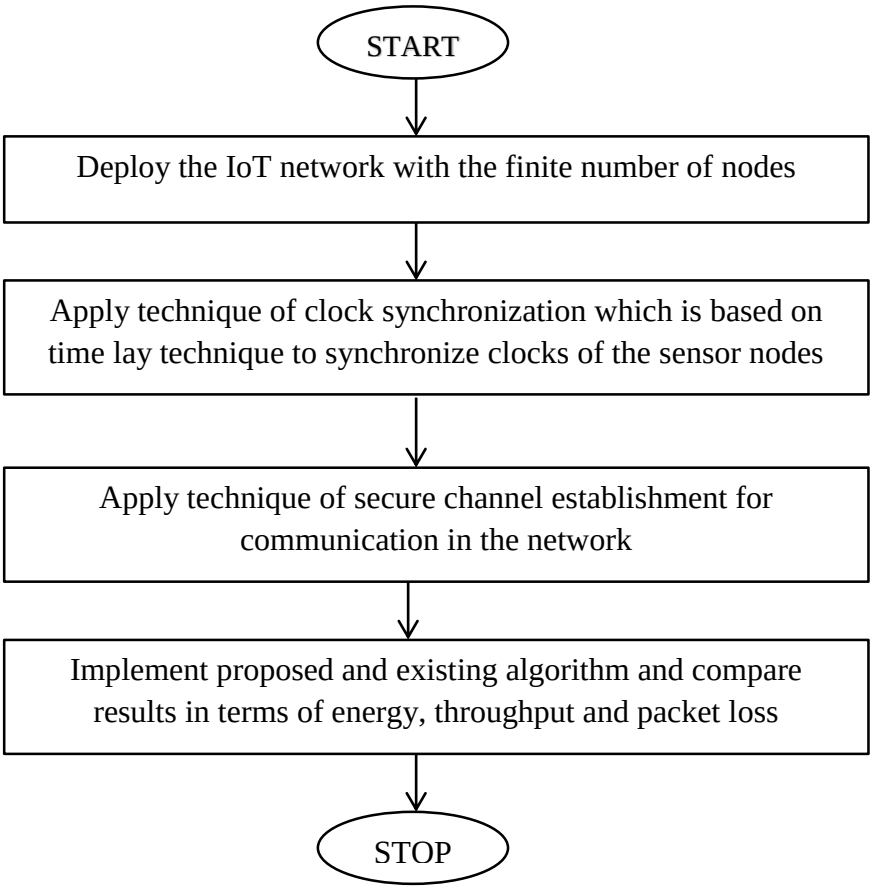

Fig. 4.1 Proposed methodology flow chart

5.1 EXPECTED OUTCOME

It is expected that the time lay technique will provide better clock synchronization and hence better security as compared to NTP based clock synchronization when implemented with respect to a specific IoT scenario. The Diffie-Hellman algorithm has more complexity than RSA due to which security of the network will be increased and also security will be increased in the network. Also it is expected that this new approach will give us better results in terms of energy, throughput and packet loss.

CHAPTER 6

CONCLUSION

In this work, it has been concluded that IoT network is the decentralized network in which mobile devices communicate with gateways and they pass the information to the applications. In the security access protocol Diffie-Hellman algorithm is applied for secure channel establishment between mobile devices and gateway. The Diffie-Hellman is complex which can be replaced with RSA algorithm in the further improvement to reduce the complexity of the network. The clock synchronization is the major issue of the IoT network. In the previous studies, NTP protocol is used for the clock synchronization which reduces network efficiency in terms of energy consumption. The time lay technique will be applied further for efficient clock synchronization with minimum delay.

REFERENCES

[1] C. Mahapatra, Z. Sheng and V. Leung, "Energy-efficient and Distributed Data-aware Clustering Protocol for the Internet-of-Things", in *Proc. of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, vol. 1, pp. 1-6, 2016.

[2] J. Yun, I. Ahn, N. Sung, and J. Kim, "A Device Software Platform for Consumer Electronics Based on the Internet of Things", IEEE Transactions on Consumer Electronics, vol. 61, no. 4, pp. 564-571, 2015.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", *Journal of Computer Networks*, vol.54, no. 15, pp. 2787-2805, 2010.

[4] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen,"*Capillary Networks – Bridging the Cellular and IoT Worlds*", in *Proc. of IEEE World Forum on Internet of Things,* vol. 2, pp. 571-578, 2015.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements and future direction", *Journal of Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[6] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," in *Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE)*, vol. 3, pp. 648-651, 2012.

[7] J. Granjal, E. Monteiro, and J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in *Proc. of IEEE on Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015.

[8] R. Giuliano, F. Mazzenga, A. Neri, A. Vegni, and D. Valletta, "Security implementation in heterogeneous networks with long delay channel," in *Proc. of IEEE AESS European Conference on Satellite Telecommunications(ESTEL)*, vol. 1,pp. 1-6, 2012.

[9] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Journal of Computer Networks*, vol.76, pp. 146-164, 2015.

[10] R. H. Weber, "Internet of Things – New security and privacy challenges," *Journal of Computer Law & Security Review*, vol. 26, no. 1, pp. 23-30, 2010.

[11] P. Wortman, F. Tehranipoor, N. Karimian, and J. Chandy, "Proposing a Modeling Framework for Minimizing Security Vulnerabilities in IoT Systems in the

Healthcare Domain", in *Proc. of IEEEEMBS International Conference on Biomedical & Health Informatics (BHI),* pp. 185-188, 2017.

[12] Z. Guo, N. Karimian, M. Tehranipoor and D. Forte, "Hardware Security Meets Biometrics for the Age of IoT", in *Proc. of IEEE International Symposium on Circuits & Systems (ISCAS),* pp. 1318-1321, 2016.

[13] T. Abels, R. Khanna, K. Midkiff, "Future Proof IoT: Composable Semantics, Security, QoS and Reliability", in *Proc. of IEEE Topical Conference on Wireless Sensor & Sensor Networks (WiSNet),* pp. 1-4, 2017.

[14] M. Mohsin and Z. Anwar, "Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics", in *Proc. of International Conference on Frontiers of Information Technology (FIT),* pp.23-28, 2016.

[15] R. Kodali, V. Jain, S. Bose and L. Boppana, "IoT Based Smart Security and Home Automation System", in *Proc. of IEEE International Conference on Computing, Communication and Automation (ICCCA),* pp. 1286-1289, 2016.

[16] V. Kharchenko, M. Kolisnyk, I. Piskachova, "Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model", in *Proc. of IEEE International Conference on Mathematics and Computers in Sciences and in Industry (MCSI),* vol. 3, pp. 313-318, 2016.

[17] A. Tekeoglu, A. Tosun, "A Testbed for Security and Privacy Analysis of IoT Devices", in *Proc. of IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS),* vol. 13, pp. 343-348, 2016.

[18] R. Giuliano, F. Mazzenga, A. Neri, A. Vegni, "Security Access Protocols in IoT Capillary Networks", *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 645-657, 2017.

[19] I. Nasr , L. Atallah , S. Cherif and B. Geller, "Time synchronization in IoT Networks: Case of a Wireless Body Area Network", *IEEE Internet of Things Journal*, vol. 14, no. 5, pp. 864-949, 2016.

[20] G. Giorgi, C. Narduzzi, "Configurable clock service for time-aware IoT applications", IEEE *International Conference on Distributed Computing in Sensor Systems*, pp. 1-6, *2017*

[21] A. Fevgas, P. Tsompanopoulou, and P. Bozanis, "iMuse Mobile Tour: a personalized multimedia museum guide opens to groups", in *Proc. of IEEE Symposium on Computers and Communications (ISCC),* pp. 971-975, 2011.

[22] Kanda, M. Arai, R. Suzuki, Y. Kobayashi, and Y. Kuno, “Recognizing Groups of Visitors for a Robot Museum Guide Tour”, in *Proc. IEEE 7th International Conference on Human System Interactions (HSI)*, pp. 123-128, 2014.

[23] N. Yu and Q. Han, “Context-Aware Community Integrating Contexts with Contacts for Proximity-Based Mobile Social Networking”, in *Proc. of IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 141- 148, 2013.

[24] Guo, D. Zhang, Z. Wang , Z. Yu, and X. Zhou, "Opportunistic IoT: Exploring the Harmonious Interaction between Human and the Internet of Things", *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1531– 1539, 2013.

[25] H. Lin, “Applying location based services and social network services onto tour recording”, in *Proc. of IEEE International Joint Conference on Computer Science and Software Engineering (JCSSE)*, pp. 197-200, 2012.

[26] Huang, C. Lee, and H. Lai, “Energy-aware Group LBS using D2D Offloading and M2M-based Mobile Proxy Handoff Mechanisms over the Mobile Converged Networks”, *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 4, pp. 528-540, 2016.

[27] B. Guo, Z. Yu, L. Chen, X. Zhou, and X. Ma, "MobiGroup: Enabling Lifecycle Support to Social Activity Organization and Suggestion with Mobile Crowd Sensing", *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 3, pp. 390-402, 2016.

[28] Namiot and M. Sneps-Sneppe, “Social Streams based on Network Proximity,” 2013, *International Journal of Space-Based and Situated Computing*, vol. 3, no. 4, pp. 234-242, 2013.

[29] S. Jisha, M. Philip, “RFID based security platform for Internet of Things in Health Care Environment”, in *Proc. of IEEE Online International Conference on Green Engineering and Technologies (IC-GET)*, pp. 1-3, 2016.

[30] H. Sandor, G. Sebestyen-Pal, “Optimal Security Design in the Internet of Things”, in *Proc. of IEEE International Symposium on Digital Forensic and Security (ISDFS)*, vol. 5, pp. 1-6, 2017.

[31] Z. Zhong, J. Peng, K. Huang, and Z. Zhong, “Analysis on Physical-Layer Security for Internet of Things in Ultra Dense Heterogeneous Networks”, in *Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green*

Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 39-43, 2016.

[32] T. Charity, H. Hua, "Smart World of Internet of Things (IoT) and It's Security Concerns", in *Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* pp. 240-245, 2016.

[33] Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things*", IEEE Journal of Design and Test,* vol. 33, no. 3, pp. 103-115, 2016.

[34] B. Sundaram, M. Ramnath, M. Prasanth, M. Sundaram, "Encryption and Hash based Security in Internet of Things", in *Proc. of IEEE International Conference on Signal Processing, Communication and Networking (ICSCN),* vol. 3, pp. 1-5, 2015.

[35] K. Navneet, K. Rajan, "Hybrid Topology Control based on Clock Synchronization in Wireless Sensor Network", *Indian Journal of Science and Technology,* vol. 9, no. 31, 2016.