Authentication and Privacy Challenges for Internet of Things Smart Home Environment

1Riaz Muhammad, 2Dr. Samad Baseer

1Department of computer science Qurtuba University of Science and technology Peshawar, Khyber Pakhtunkhwa, Pakistan
2Department of Computer System Engineering, University of Engineering and Technology, Peshawar, Pakistan

1Riazleads@gmail.com, 2drsamadbaseer@uetspeshawar.edu.pk

Corresponding Author: Dr. SamadBaseer
Email: 2drsamadbaseer@uetspeshawar.edu.pk

https://doi.org/10.26782/jmcms.2019.02.00018

Abstract

This study is a very good approach to find the solution of secure authentication for IOT based smart home environment and its appliances. The study aims to compare the different authentication methods with respect to smart home environment and trying to identify its limitation. After analyzing the existing authentication methods its limitation and core issues then targeted the message authentication for SHE.

Presently SHE authentication is based on Exchange of six message authentication techniques in Enhance authentication and key establishment scheme 6LOWPAN (EAKES6Lo) which is advance version of secure authentication and key establishment scheme (SAKES). This authentication method cause much high end to end delay, energy consumption, overall throughput of the system, complexity and poor security approach. By simulation of EAKES6Lo and SAKES scheme found some results, in contrast to these results, there may be another solution to access any SHE lights, fans, refrigerators, air condition, geezer, door lock, microwave oven, television and water pump, HVAC control and security alarms etc remotely with better security, better complexity, minimum energy consumption, better key length, better throughput and minor end to end delay named two step authentication (TSA). The proposed model also helps to monitor accessing system by comparing security codes and its complexity.

Keywords: Internet of Things(IOT), Smart Home Environment (SHE), Version 6 Low Power Wireless Personal Area Network (6LoWPAN), Enhanced Authentication and Key Establishment Scheme for 6LoWPAN (EAKES6Lo), Secure Authentication and Key Establishment Scheme(SAKES), Two Step Authentication(TSA)
I. Introduction

IOT is the abbreviated form of Internet of Things, the two parts of the IOT, first is Internet and Internet is the worldwide system interconnecting computers and the second part is Things. IOT is the connection between different computers and devices throughout the world that uses standard Protocol like TCP/IP to aid billions of computers at the same time. Internet is the combination of internetworking different computers and computer based devices that consist of billions of private, public and governmental networking devices and technologies. Now a days more than 150 countries linked together exchanging their data/Information, news and expert opinion via internet. As per the Internet world statistics more than 2.4 billion users use internet. It means that more than 38% of the world population use internet.

The second part is “things” which represents persons or objects. Things may be living things like human, animal and plants and may be non-living things like car, air conditions, refrigerators, laptops, mobiles, lights, aircrafts, ships, medical apparatus, water pumps and other home appliances, in short things are real object in this world.

Mostly internet of things (IOT) plays an important roles in modern world and vast areas with respect to network different environment of the country like city, home, industry, vehicles and all the electronic appliances. The vitality of this kind of network which connects all the devices, appliances, equipment and machines it will produce enormous benefits for human. Through IOT it will be observed that the dramatic changes will occur in world class life style of humans. We studied IOT concepts and found some limitation and security issues in different areas of it [X].

In the recent decades IOT technology gain adhesion to describe and establish a connection among different devices including industrial machinery, different electronic equipment or home equipment via Internet. From the past some years, use of electronic devices and home applications from microwave oven to satellite and airlines has become abundant. By connecting these device to the internet, we can achieve the best evolution in IOT and IOT based devices / appliances [I].

There is no standard definition of IOT because different persons like researchers, doctors, engineers, technologist, practitioners, corporate people and common man define the term according to their first use. After studying all these definitions we can say that:

“All intelligent objects connect each other and form a complete and open network that can be auto-organized, auto reacted and bear auto changes in environment”

IOT is the structure of network enabling any object any time any place connectivity, and also be a part of global network by assigning a unique identity to each and every object performing accurate communication. We can observe that in our existing network between computers, servers, switches, bridges, routers, tablets, telephones, mobiles and smart phones can communicate with each other through efficient sensors. In IOT these sensors are embedded in different physical objects for auto communications with the same IP and medium either wired or wireless. Any device or object becomes a tool to understand complexity and response quickly when they sense the environment and communicate both[XI].
The European Commission has introduced IOT and supported by The Alliance for Internet of Things Innovation (AIOTI) as a core work program. The AIOTI admits that IOT will be really responsible for upcoming troublemaking. The main objective of AIOTI is the creation of a vigorous European IOT ecosystem to set free the ability of IOT [II]. In early 2008, US National Intelligence Council (NIC) analyzed and planned that in 2025 IOT as one of “six technologies with capacity influenced on US benefits”[VIII].

The debate is still in progress in different societies that the impact of IOT and its adaptation for the next years. The different areas of IOT are smart city, IOT industries, Home appliances System, and Smart Home Environment (SHE). It is very clear that IOT will be used in all areas of life and I think the most important area is smart home.

In all the areas of the computers and PMD networking, security and privacy are the core issues for trusted IOT based system operations. The important principle which takes place in IOT is innovative security to secure system. The smart home is very easy ad hoc system, which is handled by householder without any system management and technical knowledge but it can leads specific challenges of security and privacy.

**Smart Home Environment (SHE)**

In recent years there have been a growing interest among information and communication technology (ICT) consumers in smart home Environment (SHE) concepts. This concept is appeared in the beginning of 20th century [III]. SHE vision only become possible due to the enhancement of recent development in information and communication technologies (ICT). The concept of SHE is closely related to the daily life Home Automation. Through the IOT technologies a user remotely access the home appliances and can be handled and fulfilled its requirements. A man can access and control the functionality of the air condition, geezers, refrigerators; microwave oven, television and water pump and other household electronic devices remotely. Suppose a man flies to London from Peshawar city and forgets to switch off all home electronic appliances, so he can control the appliances through SHE functionalities.

Smart means intelligent and automatic respondent, so the device having a sense to apply any activity and operation without human interaction is the key feature of the SHE. SHE function addresses high level goals like increasing comfort, reducing operational cost, guaranteeing security and privacy to householders.

We found that SHE is newly established very important area of computer science. Computer network, embedded system and applied computing form SHE. Specially the term “Smart” indicates application of various intelligent devices for enhancing the performance of home environment[III] . In other words SHE has an expert system or artificial intelligence to some extent.

Many researchers already published different articles regarding Smart city environment, Industrial Machines network and SHE privacy Issues. And it is needed to improve the security and privacy issues of SHE[VI].
Cyber Security and Privacy (CSP)

The internet technology is growing rapidly and it is the need of human life like other fundamental utilities as electricity, water, sun light and food. Internet has become a basic need of the human to search and use the health tips, educational tips, social and languages needs, kids also use internet for entertainment and online games. Different officials used internet for business, marketing, advertisement, publicity, banking transaction, funds transfer and other services. The interconnecting nature of the internet means the internet may effect from any location of the world by hacking or cracking, and this makes cyber security and privacy the key issue. This security and privacy can be achieved through Confidentiality, Authentication, Integrity, Availability, non-repudiation and Authorization.

Authentication

Computer system, computer network and its data are valuable and important, which needs to be protect. For this protection the first step is to identify or verify the user and this verification and identification of the user is referred as user authentication.

Authentication is a process through which user is verified by providing password, security token or biometric identification.

Authentication process provides the basis for access control to the computer network system.

Authentication can be used to verify the identity of user. Once user verified then access control granted to the user. The legitimate user can access the data as well as system resources [VII].

Authorization

The unauthorized access to the appliances and smart home environment controlling is a big challenge for users [VI]. And need to improve the Authentication of the Smart home environment Appliances. The question is how to improve the Authentication of the smart Home Environment to tackle authorization?

Confidentiality

Confidentiality refers as the protection of information from unauthorized released. Confidentiality means only legal users and devices can access the secure data. We know that Cryptography is a technique to achieve the confidentiality. The security and privacy may be damage through unauthorized released of confidential information. Loss of public confidence, embarrassment, or legal action against the organization could be faced, because of unauthorized release of information.

Integrity

Integrity is the type of security, which can protect data or information from rude updating and modification. Integrity is lost if unauthorized users change the data and information. Similarly the complete system will get down because of inaccurate results and online fraud.
Availability

Availability is the most important factor for any organization when it needs the online data and facilities but not available on time which cause damage to organization mission. Availability factor also affects system performance like response time delay and denial of services (DOS).

Authorization

Authorized means configure integrity that what type of permission user can use. Authorization is the type of security, which can control specification for a given system as well as allow actions for that system. (e.g., Database Administrator or authorized user decides the access rights for online users).

Non repudiation

An entity made any claim and there will be some assurance and proof that verify its truthfulness is called non repudiation.

The data integrity, confidentiality, authorization and authentication can be achieved through internet protocol security (IPSec) suit.

IOT Application Domain

Through IOT technology different application domain improved the productivity. The network of medical instrument and health equipment dramatically improve the capabilities of diagnoses a disease and finalize the treatments decision[VI]. It provide a specialist and expert opinion for rural and remote medical clinic through its interface.

IOT also plays a great role in the automobile network and looking forward for communication between automobiles, vehicle and infrastructure[VI]. Security, Cost and standardization are the important and major issues.

There is a disruptive impact of IOT on industrial equipment, public transport, sports, telecommunication, industrial production, guest houses and rest houses, education and robotics. In all of these areas, IOT is the key enabler success and mostly industrial investor are interested to invest in this new IOT technology.

Specialists and competent IT supporters ensure the security and availability of their system, so it needs to ensure the sufficient security for their organizations [VI].

IOT and SHE (Smart Home Environment)

Smart home is the newest environment as compare to traditional home environment. There is a lot of innovations in IOT based Smart home technology as compare to an existing traditional home. As we know that there is no operational phase of the IOT implementation in SHE.

There are so many Smart home Appliances which can be connected and controlled through IOT technology, and this can be possible by using Wi-Fi, Wi-max, Bluetooth, Ethernet and Zigbee with its protocols. The Smart Home provides additional security and comfort. For Example Air condition, microwave oven, water
pump, electric geezer, refrigerator and other web based household sensors be controlled through IOT technology.

**Security threats in Smart Home Environment**

**Threats**

Smart Home environment (SHE) is completely different environment as compare to other environment but the security and privacy issues are same.

i. Confidentiality is the type of security threat that caused the unwanted released of confidential information. Loss of confidentiality in Smart home environment monitoring systems may release sensitive and confidential data and other information such as home temperature, air conditional operational parameters, and other PMD devices operational parameters will lead to unauthorized access threats.

ii. Authentication is the type of security threat, to tempered sensitive and controlled information.

For example unauthenticated user gain access to the SHE lead to puzzle household controller to think that there is an emergency situation to allow an emergency exit[IX].

iii. The greatest threat is Access threat means that unauthorized access to a system controller may damage system security and privacy. This can occur through the tempered password or by unauthorized SHE accessing. If user cannot gain access through fake password and unauthorized PMD connectivity to the network, it can steal the bandwidth and leads to denial of services (DOS) to legitimate users. The denial of services may be energy reduction because many Smart home devices are battery operated[VII]. Different threat sources, motivation and thread actions.

**Vulnerability:**

Vulnerability is a security issue which targets the system resources. Mostly devices are controlled by a micro controller and these devices having limited computational and storage resources need complex security algorithms.

Vulnerability can be created from system heterogeneity. Different devices are manufactured by different companies with different network standers and software updates capabilities. There are no documentation about security and operating system in these devices. Fixed firmware is another vulnerability issue.

Slow acceptance of standards is vulnerability. Some systems have well designed standers security, such as heath monitoring sub-system. And few of them are implemented by Smart home devices.

Experts consider the largest vulnerability, which is lack of dedicated security. Experts who can manage the difficulties of a Smart Home network have to be considering this vulnerability. Only some householders can pay to professional continuing home network management assistance Instead of unprofessional one[IX].

**Existing Security Support for IOT**

Conventional computers like laptop and desktop computers are very powerful as compare to the IOT computing devices due to their low cost, low energy and limited memory. IOT uses a low-end microcontroller, such type of controllers are compatible
to the mandatory requirements. These traits moved us toward networked IOT, but existing internet protocol is not designed for these controllers which is more challenging\[VI\].

Many internet engineers are grouped together to confront these challenges. Internet Engineering Task Force (IETF) worked on IOT, to develop a unique communication protocol and performed a fundamental role for better controlled SHE and other environment over the existing IP network. These include IPv6 over Low-Power Wireless Personal Area Networks (6LOWPAN)\[V\], IPv6 Routing Protocol for Low power and Lossy Networks (LLN) and Constrained Application Protocol (CAP).

**Security existing solution for Smart Home Environment (SHE)**

Smart home environment needs a powerful security from unauthentic access of smart home equipment and appliances.

The given solution for security issue is divided into two phases.

i. System Setup

   ii. Authentication and key establishment

**First Phase:**

In first phase the given method is Advance Encryption Standard (AES), and to verify the data integrity, Message Digest Algorithm based on hash function, or secure hash algorithm is applied\[XIV\].

1. **Message Digest Algorithm (MD5)**

   It is based on cryptographic hash function which is developed by Ronald Rivest. The digest length is 128 bits and block size is 512 bits.

2. **Message Digest Algorithm (MD6)**

   This algorithm is used for security applications and check data integrity. MD6 decrypted tool is used to convert the MD6 hash to word. Its working is MD6 hashes stored in our database. When user enter the MD6 hash, our software search for hash in our database and shows its decrypted state\[XII\].

3. **Secure Hash algorithm**

   Secure hash algorithm has so many versions. The latest one has the value length is 256 bits and 512 bits.

4. **Advance Encryption Standard (AES)**

   Advance encryption standard (AES) is high efficient and secure encryption / decryption algorithm in term of time, speed, throughput and jitter. It is a symmetric key cryptography to protect the sensitive information. It is very strong against different types of attack and its complexity leads to more security.

**Second Phase**

In second phase six messages will be exchange for the fulfillment of mutual authentication in SHE which is proposed in EAKES6Lo scheme.
We focused the second phase for powerful security of Smart Home Environment and this is our core research problem, which will be discussed in coming chapters.

### Appropriate SHE Architecture for Security

There are three most important Smart Home Architecture.

1. Middleware Architecture and security
2. Cloud Architecture and Security
3. Gateway Architecture

#### I. Middleware Architecture and security

Intermediate software layer is achieved integration of heterogeneous devices that is called Middleware architecture. It is responsible for device driver interfacing and interoperability.

#### II. Cloud architecture and security

Mostly researcher proposed cloud based solution for IOT devices to solve its performances. But the collaboration between IOT devices need high processing power which is not capable of the IOT. Data Monitoring, data collection, data storage and data processing are the resources of IOT. The smart home control can be achieved by analyzing this data and by trigger cloud action according to the user policies.

   Every phase process stage logic includes event handling, thread pool and incoming event queue.

   This architecture is used in lightweight DTS[XIII] as a security protocol for communication and authentication.

   Different policies are managed by home Management system (HMS) and also provides devices access to the legal users.

   With cloud services HMS functions and interfaces are implemented. This scheme is assigned a unique key to each smart object to employ the symmetric key and encryption to apply privacy between communications. So cloud based solution provides a right direction for IOT connection and cooperation instead of typical solution.

#### III. Gateway Architecture

Gateway is the bridge between IOT infrastructure and cloud. Gateway has more resources and computational ability. Rich memory and high computational power can be offered from the IOT to the gateway.

   It is a guard against the unauthorized users to modified data and can also protects smart devices from cyber threads.

   In literature [IV] the authors presents Integrated Access Gateway (IAG) architecture to support various applications of SHE. It is also implement the security issues such as authentication, authorization and encryption. The important benefit of this architecture is Quality of services (QOS).
A gateway server proposed by Server Based Internet of Things Architecture (SBIOTA) which provide a better and secure integrated solution to SHE.

Upcoming SHE Challenges

My research is based on currently investigating, enhancement of gateway based architecture security. My approach is in early stage so I present overall system architecture and its problems. In SHE environment householder face many problems, errors and challenges to achieve secure communication just because of deficiencies in technical support. Householders and experts need to study secure auto configuration approaches for successful implementation of smart home environment (SHE).

The security approaches in Smart Home Environment (SHE) are quite different from IOT industries, medical equipment and other utilities.

Auto configuration Support

A device when come under a network need cloud based functionality, these functionalities investigate device details including ID, commands, encryption standard, protocols and firmware updates which makes it trusted. Information is up to date between these devices and web through this simple approach.

IOT software updates

Through it secure vulnerabilities are found and repaired, the desktop system software are updated automatically. PMD or PDA also receive software updates regularly to verify the authentication, such systems are inexpensively feasible because number of manufactures are limited and target deployed PMD devices are in millions. No such updates are available for thousands of IOT devices.

IOT devices are the collection of hardware and software to perform specific activities. There is a software named Firmware into the PMD or PDA, which is an important part of IOT. System activities and functionality are controlled, from device initialization, users interfacing, request processing and task performance.

It is also very important that the smart home device firmware is the latest version to resolve the security vulnerabilities and improved functionalities as well as add new feature.

IOT based devices should have a very good mechanism to implement safe and secure firmware updates automatically without user intervention. Certificate based digital signature should be applies for the updates to ensure the authentication of the updates and protect firmware tempering such as malware attacks. Before updating software each update should be verified against its digital signature and this digital certificate should be examined its validity issued by the third party or vendor.

An attacker can costume the legitimate previous firmware versions, update its security vulnerability as the updated version, if the update checking mechanism are compromised.

Therefore the device manufacturers should encrypt and digitally signature update release information. We know that the limited resources and low bandwidth nature of many PMD or PDA improve efficiency and reduce the installation time which may reduce the possibility of update failure.
According to author that such architecture GITAR has the ability to use standard structure and methods to apply application protocol during run time[III]. It compromises of following levels:

i. Static system levels

ii. Dynamic components level

iii. Kernel level

IV. Literature Review

In 2006 Mr. Mangal Sain, Mr. Young Jin Kang and Mr. Hoon Jae Lee from Department of Computer Engineering, Dongseo University, South Korea found that IOT is the embedded with internet of all electronic devices, sensors, actuators, and network connectivity. IOT requires customized security and privacy. IOT involves in different communication technologies which require a common communication standard. The main objective of this survey paper is to provide a better understanding security approaches in IOT models and discover what challenges need to make secure communication in IOT.

In 2010 Atzori, Luigi, Iera, Antonio, Morabito, Giacomo observed that IOT has changed radically. IOT creates a very good connection between people and devices in several circumstances, traversing data and information from professional life to social associations. The IOT has the ability to add new dimension by enabling communications among smart objects. Thus IOT achieving the vision of “anytime, anywhere, anything” communications.

In 2012 Lei Yu, Yang Lu, XiaoJuan Zhu from School of Computer and Information, China analyze smart hospital’s architecture its key technology and construction. They also suggest implementation of smart hospital. They propose a concrete application scheme for smart hospital and changes in the existing hospital model, to achieve satisfactory result. They also describe related research on mobile electronic medical record and overall implementation of smart hospital.

In 2014 Komninos, N., Philippou, E. &Pitsillides, A. Members of IEEE investigates the security issues related to the SHE by focusing several scenarios of the most representative threats. The threats detected and categorized according to specific security goals set for the Smart Home environment and their impact on the overall system security. In this paper they presented dangers threatening interaction amongst entities of Smart Home environment. They have also found different approaches to protect and block different attacks to achieve the security objectives.

In 2015 Somayya Madakam, R. Ramaswamy, Siddharth Tripathi observed that IOT convert the real world objects into intelligent virtual objects. The IOT giving us a complete control on devices and things around us as well as informed us about things and devices. IOT is technological uprising that represents future of Information and communication technology, and its development depending on dynamic technical innovation. IOT bringing great changes in our daily life, which helps to make our life simpler and comfortable. There are so many advantages of IOT applications in all
The key observations in this paper is:

1. No standard definition worldwide
2. Universal standardizations required
3. Need standard protocols

In 2015 Yue, Q. and Maode Ma, Senior Member of IEEE investigates that message authentication plays a vital role in M2M communication. There are two phases of M2M communication, first one is authentication phase and second is key establishment phase. To enhance the secure functionality of Machine to Machine communications in 6LoWPAN networks, EAKES6Lo scheme has been proposed. The security analysis has shown the EAKES6Lo scheme is more secure and can successfully prevent various malicious attacks. Therefore, Yue and Maode proposed 6 message authentication techniques in EAKES6Lo scheme for smart home environment.

In 2016 Huichen Lin and Neil W. Bergmann from School of IT and Electrical Engineering, Australia found that different securities issues of IOT is a single domain for Smart home environment. There are a huge difference between sensitive commercial operations and domestic smart home environment for the need of privacy and security. Cyber security revolves Confidentiality which keeps data private, it means only authorized and legal users can access data and authentication process verified that the data is tampered or not. However, securities issues are very similar to all other domain although SHE is a completely different environment. The author writes that a security threat in Smart Home is Confidentiality and unauthorized user can access data due to loss of confidentiality. The Authentication threats can protect sensitive information from unauthentic user. The Vulnerabilities is another security issue that is come when SHE under malicious attack because of system deficiencies.

In 2016 Ding, F. Song, A. Tong, E.;Li,J evaluated different architecture of smart gateway, and investigates different scenarios to access smart home appliances. In 2016 Alam Hossain, Biddut Hossain, Shafin Uddin, Shariarand Imtiaz concluded that MD6 is an encryption algorithm which keeps very important contribution in network security. This paper analyzes the performance of commonly used encryption techniques and algorithms like AES, DES and RSA. It is concluded that there is a big difference between AES and RSA algorithm because AES consume less and RSA consume more encryption time. In this paper it is also concluded that decryption of AES algorithm is better than other algorithms.

In 2017 Costin Badic, Marius Brezovan and Amelia Badic from University of Romania writes about smart home environment its architecture, application and technology. They observed that smart home closely related to the more established area of Home Automation. They also studied the detection, signaling, alarming, monitoring, security violation and response of smart home. They identified number of security issues that must be considered for SHE.
In 2017 Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah from School of IT and Engineering, Canada suggested an improved authentication scheme for WSN. The author finds security analysis and evaluation, that their protocol is very strong and secure as compare to the existing schemes.

After the study of the above literature, it is summarized that SHE authentication needs better solution as compare to the SAKES and EAKES6Lo. IOT based SHE used 6 message authentication which has some flaws. The literature provides me a complete knowledge about IOT, SHE, network security, security algorithms, security protocols and TSA. Really no of scientist, researchers and experts had done a tremendous job on the desire issues.

The previous authentication schemes SAKES and EAKES6Lo exchange 6 message for secure authentication which causes end to end delay as well as minimum security for SHE. Again check the delay Time through mat lab simulation which is 6s and 7s consecutively and similarly the authentication approach is also an old method, it needs to use the newest authentication techniques like Two Step Authentication (TSA).

V. Results

Proposed model

Proposed model based on two step authentication:

Algorithm Steps

I observe different aspects of SHE and finalized the authentication issues for SHE. In the below diagram any unauthorized user can gain access to the SHE and misuse it. So we propose out new model for SHE authentication.

Anybody can enter your user id or password then the web site or server asked for a special code that can be 6, 8 digit code through sms, email or through any apps.

A cellphone or PMD request for accessing the smart home appliances the home gateway ask for special code which can be 6 or 8 digits, from register cellphone or PMD. The home gateway checks the PMD and code if matched then the authentication will be granted if not matched then a sorry message will be sent to the requisite.

1. A device requests for authentication from server by providing user Id and password.
2. Server check the user Id and password as one step authentication.
3. Server broadcast a message to register cell no or PMD and ask to enter a special code (that can be 6 or 8 digit code which is already in listed with home gateway)
4. User sends the code to the server.
5. Server check the code with the listed code information, if matched to the existing then authentication will be granted otherwise sorry message will be sent toward the requisite.

**Time factor**

The Figure 1 given below shows the delay status in SHE Authentication on different node. It is clear from the graph 1 that the Two Step Authentication (TSA) has less delay as compare to EAKES6LO and SAKES, so that’s why Two step authentication is highly recommended for SHE.

The simulation results clearly indicate that two step authentication has less time consumption in SHE authentication and this is the requirements of the IOT based SHE now a days.

So I proposed Two Step Authentication (TSA) instead of EAKES6Lo and SAKES in light of delay factor.

**Time Factor on Server**

The below Figure2 show that the total time delay is less as compare to EAKES6Lo and SAKES, because both previous schemes exchange 6 messages for authentication, which cause time delay on server side. so this new model shows better results in Mat lab simulations.
To enhance secure issues of the SHE, the Two Step Authentication (TSA) scheme is designed for secure SHE. It consists of three phases:

1. Pre-deployment phase
2. Authentication phase
3. Handover phase.

Assume that all devices have short unique address 16 bit to 64 bit using 6LOWPAN protocol, and create links between PDA and PMD and server is secure.

The proposed Two Step Authentication (TSA) model is analyzed from three aspects.

1. A proof of the logic correctness will be provided to model that two step authentication (TSA) model fulfill its corresponding security issues.
2. A formal verification is taken to automatically verify the security functionality.
3. Finally further analysis, explanation and the ability against various malicious attacks of the proposed solution are provided.

The Figure 3 shows the protocol analysis results and clearly indicates that TSA is better than the previous EAKE6Lo and SAKES.
As a result, total computational overhead of Two Step Authentication is much better as compare to EAKES6Lo and SAKES, as we know about the delay Time 6.24 s and 7.407 s, for SAKES and EAKES6Lo respectively. Though Two Step Authentication is proved to be quick and safe as claimed.

The model consist on three basic phases:

i. Registration Phase

ii. Sign in and authentication Phase

iii. Password update &change Phase

**Complexity:**

Two type of complexity is focused in this study. The proposed solution provide minimum time for accessing the required device and also provide enough security. As compare to previous solution for device authentication, TSA has the ability to tackle time complexity. In SAKES and EAKES6Lo has some flaw as code complexity and TSA provide hexadecimal code complexity, which increase accessing security.

**Figure 3**

![Total Time Delay of the Protocol](image-url)
Energy Consumption:

Energy is a major issue in PMD and PDA which may need to solve. EAKES6Lo exchange 6 message for authentication and these 6 messages involve system 6 times which cause more energy consumption as compare to TSA. TSA only sending request and receiving authentic code. As authentication and privacy concern TSA is more reliable to control energy consumption for SHE.

Key-Length:

Some existing two step authentication uses 16 bit key length for security codes but in SHE the model proposed 32 bit hexadecimal code to solve authentication and privacy challenges. 32 bit key length is sufficient for this model, but it may vary with the passage of time or it may be observe time to time.

Throughput:

Amount of data transmission in per unit time is throughput, so the unit of throughput is bits per second (bps). In TSA there is no a lot of data transmission over the network, server only request to the authentic user to prove a security code and authentic user send an authentic code toward server then server compare security codes and grant access the requisite user. In EAKES6Lo the no of hits to the computer is 6 which effect the throughput of the network and in TSA the no of hits to the computer is reduced and handled the throughput of the network.

VI. Summary:

If a person wants to gain access to SHE remotely through internet securely, then we need two step authentication (TSA).

For example I am traveling form Lahore to Peshawar and I want to gain access to my home and handle different home appliances and devices to save my time and efforts, so this is a very good solution to create IOT based SHE. Similarly to handle the SHE securely within a short Spun of time then we use TSA. Different authentication is used in SHE but these authentication have different flaws, so I proposed Two Step Authentication (TSA) proposed for SHE. Because of minimum end to end delay and the newest authentication techniques.

VII. Conclusion

The thesis concluded that in smart home environment where secure authentication needs to access devices and appliances, the existing 6 message authentication in SAKES and EAKES6Lo resulted 7 second delay for each object accessing, and security issue still in presence then the only way to tackle the better security for object accessing in minimum time is two step authentication (TSA). In two step authentication dual check confirm the authorization of the authentic user. In first step it checks the user identity with user name and password and in second step server requests for verification code which is sent by server on user registered PDA or PMD device, if the code matched authentication will be granted otherwise authentication will be denied.
VIII. Recommendations

- This study recommended the two step authentication for internet of thing smart home environment instead of 6 message authentication of SAKES and EAKES6Lo.
- Two step authentications have several methods, and different special devices are used, but recommended TSA is message authentication.
- Recommends 6LOWPAN for Two step authentications (TSA) as used by SAKES and EAKES6Lo
- This study was conducted using simulation tools Mat lab, so it need further analysis for precise results.
- The two step authentication evaluated to implement security in SHE, so keep in mind about two step authentication main objectives.
- Only parameters privacy, security and delay should be determined for proper functionality of IOT based SHE.

References

I. Atzori, L., Iera, Antonio, Morabito, Giacomo, The internet of things: A survey. Computer networks, 2010. 54(15): p. 2787-2805.

II. Commission, E., The alliance for internet of things innovation (AIOTI). 2016.

III. Costin Badică, M.B., Amelia Badică, A., An Overview of Smart Home Environments: Architectures, Technologies and Applications. 2017: p. 8.

IV. Ding, F.S., A.; Tong, E.; Li, J., A smart gateway architecture for improving efficiency of home network application. 2016.

V. Geoff Mulligan, M.y., Patrick Wetterwal, Colin Patrick O'Flyn, Making sensor networks IPv6 ready. 2008.

VI. Huichen Lin, N.W.B., IoT Privacy and Security Challenges for Smart Home Environments. 2016(4 July 2016).

VII. Internet, ADVANCE AUTHENTICATION TECHNIQUES.

VIII. Kenji, I.M., T.; Toyoda, K.; Sasase, I, Secure parent node selection scheme in route construction to exclude attacking nodes from rpl network. 2015. 4: p. 5.

IX. Komninos, N., Phillippou, E. & Pitsillides, A ., Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures 2014.
X. Madakam, S., R. Ramaswamy, and S. Tripathi, Internet of Things (IoT): A Literature Review. IT Applications Group, 2015 3: p. 164-173.

XI. Mangal Sain, Y.J.K., Hoon Jae Lee, Survey on Security in Internet of things: state of the art and challenges 2014.

XII. Md. Alam Hossain, M.B.H., Md. Shafin Uddin, Shariar Md. Imtiaz MD6 Message Digest Algoritham. Reasearch Gate, 2016. 16.

XIII. Rescorla, E.M., N., Datagram Transport Layer Security. Internet Engineering task force, 2012.

XIV. Sandeep Kumar Rao, D.M., Dr. Danish Ali Khan, A Survey on Advanced Encryption Standard 2017.