Analysis of Security methods in Internet of Things

Saranya. C. M
PG Scholar, Dept. Of CSE
Vidya Academy of Science and Technology
Thrissur, India
saranyamathukutty@gmail.com

Nitha. K. P
Asst. Professor, Dept. Of CSE
Vidya Academy of Science and Technology
Thrissur, India
nitha.k.p@vidyaacademy.ac.in

***Abstract*—** Internet of Things (IoT) is a new revolution for the internet. IoT is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service. In addition, the Internet of Things can be providing variety applications via convergence with other technology such as machine-to-machine, Wireless Sensor Network, and Web technology. In this paper describes the analysis of security methods in the area of IoT and also describes a protocol which combines zero knowledge proof and key exchange algorithm to provide secure and authenticated communication that can be applied in IoT environment.

Keywords-*Internet of Things (IoT), GMWZKP, Security methods in IoT, Applications*

*****

I. INTRODUCTION

The IoT may be a hot topic in the industry but it's not a new concept. Internet of Things is a new revolution of the Internet. IoT describes a system where items in the physical world, and sensors attached to these items, which are connected to the Internet via wireless and wired connections, sensors are used for collecting information. The Internet of Things vision is to successfully emerge, for connecting everyday existing objects and embedding intelligence into our environment. The automatic exchange of information between two systems or two devices without any manual input is the main objective of the IoT and it gives a new dimension to the world of information and communication. IoT have security threats, while exchanging information. Different types of security frameworks are used in IoT. The IoT also ensures the confidentiality, integrity and authentication that finds inevitable role in Zero Knowledge Protocol (ZKP). It is an advanced protocol which ensures data integrity, confidentiality and authentication. IoT introduces new challenges for the security of systems and processes and the privacy of individuals.

Different security methods are used in internet of things for providing security for communication, authentication, data sharing etc. For providing higher security in IOT zero knowledge protocol is used. Zero-knowledge protocols allow identification, key exchange and other basic cryptographic operations to be implemented without leaking any secret information during the conversation and with smaller computational requirements [5]. Thus Zero-knowledge protocols seem very attractive especially in smart card and embedded applications. To attain high security in ZKP we have to set the secret as hard as possible.

A method for peer-to peer authentication and encryption based on the Goldreich-Micali-Wigderson (GMW) graph isomorphism zero knowledge protocol and the Diffie-Hellman key exchange [1] is a promising approach that can be implemented on the small embedded systems. Embedded systems are becoming increasingly vulnerable to masquerade and replay attacks due to increased connectivity, creating a need for authentication. Different authentication schemes are used in embedded systems for providing security and unauthorized access.

Network security is a critical requirement in emerging networks. The purpose of network security, quite simply, is to protect the network and its component parts from unauthorized access and misuse [3]. Network security is provided by the internet protocol Transport Layer Security (TLS). TLS is the successor to the Secure Sockets Layer. TLS is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. This approach is implemented for small devices using IOT.

II. INTERNET OF THINGS

Internet of things (IoT) or Internet of Everything (IoE) is extension of new generation internet technology. IoT defines that the networks of physical objects that contain embedded technology to sense of interact with their internal state or external environment. It comprises an echo system that includes things, communication, applications and data analysis. It has the ability to connect a device to network that sends information from one device to another device. For secure communication need authentication in devices. Devices which are used in the IoT environment should require IPV6. A fully integrated IoT platform delivers the data analytics capabilities as well as the end to end security for encryption of data, users and devices. IoT is secure standard based and scalable platform.

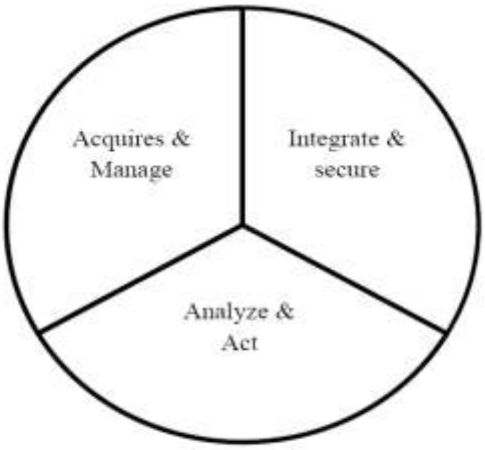

Figure 1: Architecture of IoT

The first part in the architecture is acquiring and managing data. That is collecting the individual data points using sensors. The second part is Integrate and secure. Integrating data receives from various components and devices. The third part is analysis. Internet of Things systems must have the capability to discover, store, and analyze tremendous amounts of data in all formats, and then be able to communicate [4]. There are four key technologies describes in [14]. They are smart technology, sensor network, nanotechnology, RFID.

III. ISSUES AND CHALLENGES IN IOT

Get Data Securely to the Right Place, at the Right Time, in the Right Format [4]. There are many opportunities to extract value from the data generated in the connected world, but the rapid growth in the number of intelligent devices presents many challenges, and has a significant impact on the architecture of IoT services [7]. Major security issues in IoT are privacy, confidentiality and authenticity, for ensuring confidentiality, a large number of standard encryption technologies exist for use. However, the main challenge is to make encryption algorithms faster and less energy-consuming. Moreover, an efficient key distribution scheme should be in place for using an encryption scheme. Security issues can be considered in two domains they are Security domain and user domain. Security domain provides security in the architecture of IoT in design and execution time. And also protect from arbitrary attacks and malicious software. In the domain of user the specific challenges are data privacy and control over individual's physical location and movement. Attacks in IoT are physical attacks, side channel attacks, software attacks, network attacks, environmental attacks etc.

Physical attacks based on hardware components, Side channel attack related to side channel information, Wireless communications are vulnerable to network attacks.[6] Low power embedded devices have a big challenge in security, because the computation power is limited for these devices and insufficient for processing of higher computation security algorithms like RSA,AES,DES etc.

IV. SECURITY METHODS

Different security methods are used in IoT. In [8] proposes a security frame work for mobile devices. This frame work is implemented for securing the mobile devices, which is useful in future of IOT. Frame work consists of three components. The three components are lightweight forensic application, collaborative component, and network component. Each component is designed to enhance the existing solutions. Lightweight forensics application is used for set off alarms when the data met. For this it use a set of rules and parameters. Data collected from the lightweight application is sent to the network component for further analysis. The collaborative component is used for collecting data in the distributed network and also indicates the possible attacks. Mobile devices have the ability to monitor the neighbouring devices and report if any threats are detected. After detecting threats they can send warnings to those devices. IoT provides good opportunity for using collaborative threat detection in devices in the distributed network. Network component uses a central security manager for the processing and resources for the data sent by the lightweight application and collaborative component. Using this frame work can detect the attacks and react to attacks. But this is not an end product for the security of IOT.

IoT is applied in medical environments. To provide security in medical field [9] proposes a method. When applying IOT in medial environments, the problems are raised due to mobility and security. The goal is that global connectivity in medical environments to provide patients life easier and the clinical process more effective. The propose idea is going to implement a set of security techniques and SIM card for authentication, encryption and sign the communications with mobile devices. The main goal of this architecture is related to IOT which offers AAL (Ambient Assistant Living) services for elderly people in medical environments. The proposed architecture is based on 3 pillars. Firstly to provide connectivity to devices used .Second and thirdly are used the technologies communications. 6LoWPAN (IPv6 based Low-Power personal Area Networks) for active communications and RFID & NFC for passive communications. By using these technologies raised the problem of capacity to handle the mobility and security as in IPV6. To solve this problem include cryptographic SIM card for security and mobility as defined in IPV6. This technology provides solution for the security challenges in medical devics.

In [6] describes a frame work for embedded security in IoT. By creating a frame work we have to consider the factors cost, performance and security. This frame work provides a synthesis oriented approach to achieve security systems implementation having both hardware and software.

Lightweight cryptography, physical security, standardized security protocols, secure storage are the key features of this frame work. The frame work consists of hardware and software components with lightweight cryptographic standardized protocols. The device level of security depends on the kind of application. It provides physical protection of secrets keys by keeping the components secure. Here uses the rich operating system which maintains the necessary security functionalities. This security framework contributes good security architecture for IoT.

[10] Describes a new approach for the context of IoT for security. It consists of four nodes and tensions. Nodes are person, process, intelligent object, technological echo system. Nodes are interacting through the tensions. Three domains are used in this application. Domains are Smart environment domain, Health –care domain and transportation domain.

In [11] proposes a new approach for the authentication and communication of group of devices in IoT. The approach is Cryptography based Group Authentication (TCGA) and it is implemented in wifi environment. The proposed TGCA consist of session key in the end of the each group authentication. This authentication is done in two phases. First is pre-authentication phase and second is group authentication. Pre-authentication means that all devices should be authenticated in the group itself. Devices which are not in the member of group cannot communicate with other groups or devices. TGCA consists of 4 modules. They are key distribution, key update, Group credits generation, Authentication listener, message decryptor. It is lightweight approach in wifi environment for the authentication of devices. TGCA protected devices from replay attacks and MIM attack.

V. PROPOSED ARCHITECTURE

The Proposed architecture for security in device authentication is GMWZKP (Gold-Micali Widgerson Zero Knowledge Protocol). It is a new protocol which is introduced by Gold Micali Widgerson. The protocol is combines with the zero knowledge protocol and a key exchange algorithm to provide secure and authenticated communication that can be applied in IOT. The proposed architecture provides secure and authenticated communication in static machine-to-machine (M2M) networks and in small embedded systems by using Internet of Things (IOT) [1]. This protocol provides perfect forward secrecy. Here ZKP authentication is implementing using GMW method by using graph isomorphism. Two graphs G1 and G2 are said to be isomorphic, they differ only by the names of the vertices and edges. There is a complete structural equivalence between two such graphs. Authentication is processed by using authentication frame.

The authentication frame consist of

<IG||i||Id||Success||SOL||CHL>

Where,

IG	→	Initial Graph
I	→	Number of rounds
Id	→	Unique identifier
Success	→	Flag indication
SOL	→	Response of challenge
CHL	→	New challenge

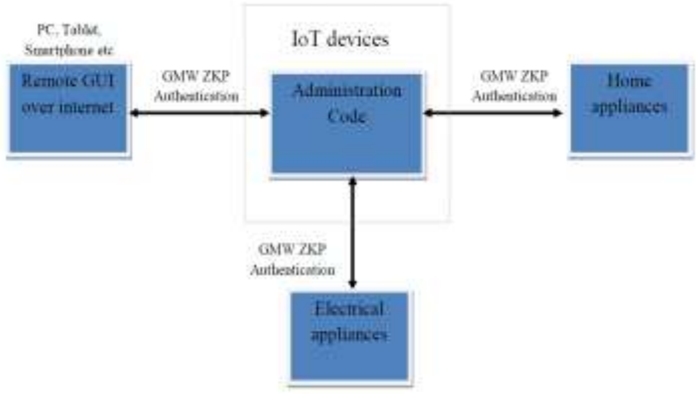

Figure 2: Proposed Architecture

The proposed system based on graph isomorphism and it is an effective authentication in small embedded systems. It resists from physical attacks, replay attacks. Architecture consists of ZKP and a simple key exchange algorithm. Simple Diffie Hellman is used in the system and it is a proved algorithm. It detects and avoids MiM attack.

A. *GMW Zero Knowledge Protocol*

The GMW protocol is based on graph isomorphism. The graph isomorphism problem is NP, as there is no known polynomial time algorithm that solves it. In the GMW protocol the prover's secret is a graph permutation π that is the isomorphism between two publically known graphs G1 and G2. Suppose there are two graphs *G1* and *G2*, such that the graph *G2* is generated by relabeling the vertices of *G1* according to a secret permutation π while preserving the edges. [12]The pair of graphs *G1* and *G2* forms the public key pair, and the permutation π serves as the private key. A third graph *H*, which is either obtained from *G1* or *G2* using another random permutation, say ρ is sent to the verifier who will in return challenge the prover to provide the permutation σ which can map *H* back to either *G1* or *G2*.

VI. APPLICATIONS

The IoT have variety of applications in the areas of vehicles, industries etc. The general application of IoT in describes in [14]. They are networking service, operational service, security service, management service. Onstar organization provides a variety of technologies for communication.

a) Delight connect is an application which is used for controlling the vehicles.
b) Parksight application is used for parking area. A sensor senses the parksight for the vehicle.
c) Informs the potential of building using IoT technology.
d) Transit is an application used for the information related to status of engine of the vehicle like bus, train car etc.
e) Elderly monitors application reminds for eating medicines for elder people.
f) Water monitors application in IoT checks the level of the water in the tank according to the usage.
g) IoT applied in agribusiness industry, if any problem in soil content, It will inform the irrigation system.
h) IoT applied in consumer goods industry for the manufacturing distribution and consumers.
i) Applications in Oil and gas industry for upstream extraction, processing and downstream distribution.
j) IoT applied in the aerospace and aviation industry to improve the safety and security.
k) IoT in pharmaceutical industry provides safety and security in pharmaceutical products by attaching label.

The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, and Factory, Supply chain, Emergency, Health care, User interaction, Culture and Tourism, Environment and Energy.[13] New types of applications can involve the electric vehicle and the smart house, in which appliances and services that provide notifications, security, energy-saving, automation, telecommunication, computers and entertainment are integrated into a single ecosystem with a shared user interface. In the future computation, storage and communication services will be highly pervasive and distributed: people, smart objects, machines, platforms and the surrounding space will create a highly decentralized common pool of resources interconnected by a dynamic network of networks.

Challenges in smart city IoT applications describes in [13]. The processing and analysis of required algorithms for the city are difficult and also required for the usage of low energy protocols and algorithms. Some IoT applications are tightly linked to sensitive infrastructures and strategic services such as the distribution of water and electricity and the surveillance of assets. Some Other applications handle sensitive information about people, such as their location and movements, or their health and purchasing preferences [2].

VII. FINDINGS

Our system is to find better authentication in small embedded systems using Zero knowledge protocol and a key sharing algorithm that can be applied in IOT. The table shows that the comparison of Security methods in the environment of Internet of Things. On theoretical study Graph isomorphism based Zero Knowledge Protocol and Diffie-Hellman algorithm provides better result for authentication in small embedded systems. Zero knowledge is powerful authentication method for authentication.

Sl N0		**Algorithms**	**Findings**
1	Internet of Things	Proposed embedded security frame work	Avoid software attacks, hardware attacks
		Frame work for device security	Effective method in mobile devices communication
		Architecture in medical environments	Effective technique for the authentication in medical devices
		Based on graph isomorphism	Effective authentication in small embedded systems. With low cost

Table 1: comparison of IoT methods

VIII. CONCLUSION

Different security frame works are used in IoT environment for providing greater security. In this paper proposes a new method which provides security, privacy, integrity and authentication among peers in static devices. It is based on Zero knowledge protocol and key exchange algorithm. The proposed architecture guarantees perfect forward secrecy. It aims low power consumption and fast computation.

REFERENCES

[1] Pádraig Flood, Michael Schukat , "Peer to Peer Authentication for Small Embedded Systems", 2014 IEEE

[2] www-journals-elsevier-com.

[3] University of Florida Department of Electrical and Computer Engineering Bhavya Daya Network Security :History, Importance ,and Future

[4] http://www.oracle.com/us/solutions/internetofthings/iot-manage-complexity-wp-2193756.pdf.

[5] Helsinki University of Technology" Zero knowledge protocols and small systems".

[6] Saching babar,Antonietta stango "Proposed embedded security frame work for Internet of Things(IoT).

[7] http://www.oracle.com/us/solutions/machine-to-machine/m2m-brochure-1951397.pdf.

[8] Helen Angela Brumfitt, Dr Robert Askwith, Dr Bo Zhou "A Framework for Device Security in the Internet of Things" Liverpool John Moores University Department of Networked Systems and security.

[9] Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta *IEEE Member* "An architecture based on Internet of Things to support mobility and security in medical environments.

[10] Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou, Abdelmadjid" A Systemic Approach for IoT Security.

[11] Parikshit N. Mahalle*, Neeli Rashmi Prasad** and Ramjee Prasad**. Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)

[12] Eric Ayeh, An Investigation Into Graph Isomorphism Based Zero-Knowledge Proofs University Of North Texas December 2009.

[13] Rivers publication seris in communication "Internet of Things:Converging Technologies for Smart Environments and Integrated Ecosystems.

[14] Miao Yun, Bu Yuxin "Research on the Architecture and Key Technology of Internet of Things (loT) Applied on Smart Grid" 20 I 0 IEEE.