Authentication and Privacy for IoT Objects: A Survey

Harish Kumar N[*1] **Deepak G**[*2]
[*1,2] Assistant Professor, Dept of CSE
[*1,2] Dayananda Sagar College of Engineering Bangalore, India

***Abstract*— Internet of Things (IoT), an emerging technology which offers capability to physical objects to hear, think and perform task by communicating and sharing the data with other physical objects. This paper discuss about IoT Architecture, user interaction with the objects, security aspects in IoT and some authentication approaches discussed in the literature to mitigate the security attacks and privacy for the objects in IoT.**

Keywords*— *Internet of Things, Authentication, Privacy.

I. Introduction

The most interesting and challenging communication technology of 21st century is Internet of Things (IoT). It is a network of different objects which are connected to internet and has capability to communicate with the other objects. The objects are termed as "Things" which can be RF-ID tags, Sensors, Mobile Devices, and any other appliances. IoT allows the objects to interact with the real world through internet anywhere and anytime. These objects possess a unique ID which is used to interact with other objects and users. The objects that interact in the real world are usually resource constraint such as lower computational power, less lifetime, low memory etc.

IoT offers wide range of applications such as Smart Home Automation, Traffic Management, Health Monitoring, Device Monitoring etc. Cost reduction in hardware and network setup, and the fastergrowth of wireless communication technologies which are quick and easy for deployments, lead to the expansion of IoT in today's world. Since the devices are accessible from anywhere care to be taken to prevent unauthorized access and violation of privacy. Other major security requirements considered for IoT are secure data communication, Identity of the object, data gathered to be kept confidential etc.

II. IOT ARCHITECTURE

The above architecture shows how the objects are connected to the network and how they interact each other to establish communication between them. The object that comes in the scenario are usually hand held devices like mobile phones, personal computers, laptops, and objects which communicate with the databases.

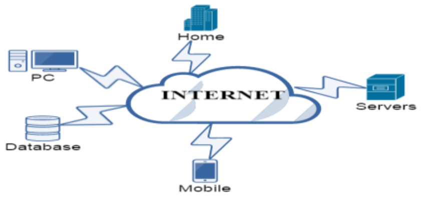

Figure 1: IoT Architecture

Living homes can be automated using sensor devices like temperature sensor, light sensor, fire sensor, smoke sensor etc. city surveillance can be made using the IP cameras. In agriculture IoT plays a vital role like soil quality measurement, humidity check in soil, watering crops in regular intervals etc.

Figure.2 shows how user interacts with objects providing authentication and privacy to the objects.

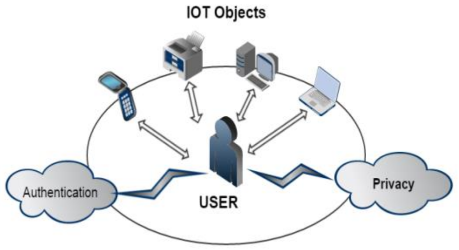

Figure 2: USER Interaction with objects

III. LITERATURE SURVEY

A brief review of literature about the authentication and privacy approaches has been carried out in this section.

Chunye Hu, Jie Zhang et.al [1] has presented an identity based system for personal location in emergency situations. The system consists of registration subsystem, policy subsystem, user authentication subsystem, and client subsystem. The framework affirms the personality of the client through the client verification subsystem and gets the dimension of the crisis through the strategy subsystem. user's location information can be accessed only by authorized user, on necessary conditions. The system reinforces the protection of the user's privacy and also providing the location of the user, and avoids the revelation of the users' information.

Swati Kinikar Dr. Sujatha Terdalet.al[2] has implemented an open authentication protocol for IoT based application user's private data that is stored on another system is used through the IoT device. Smart devices have limited productivity in terms of computing storage and battery. Due to the inadequate storage of embedded devices, it is hard to implement strong authorization techniques. Among the various authentication protocols existing today, OAuth provides a simple and secure way to authenticate the users and permit them to access the protected. A smart fire alarm system is proposed that notifies the user about any fire occurrence in the house. User acquires an alert message over his twitter and Gmail account simultaneously. Fire alarm system is built on IoT technology integrating with temperature sensing sensors. In order to access to Gmail and twitter the iot device need to authenticate on behalf of the user. This is accomplished by OAuth protocol for granting access to applications like twitter and Gmail.

ShadiJanbabaei, Hossein Gharaee, et.al[3] has presented a novel lightweight authentication in IOT Infra. In this approach, author explains how Internet of things architecture is used for modeling proposed authentication protocol. The proposed architecture includes four necessary components: an authenticated cloud server (ACS), network entities such as CH and home IoT server (HIoTS) and edge devices like SNs. Along with the architecture an authentication scheme between sensors is proposed. The proposed scheme consists of two phases. Initially it is a registration phase, which allows HIoTS to send security credential to SNs through a secure channel. Sensors are validated in second phase. The sensor devices are free to move from one cluster to another or they can be stationary in specific location.

Hokeun Kim, Eunsuk Kang, Edward A et.al[4] has presented a tool which is open-source for developing an authorization service infra for iot. The Secure Swarm Toolkit uses distributed local authorization entities, by providing authorization services which can address heterogeneous security requirements and constraints with respect to resources in the IoT. The authorization services can be retrieved by network entities through software interfaces provided by SST, called accessors. The accessors allow IoT developers to readily integrate their devices with authorization services without needing to manage cryptographic keys and operations. In addition, the scalability of the proposed approach with a mathematical analysis has been presented.

Yong Jin ,MasahikoTomoishi, et.al[5] has designed a Secure and Lightweight Device Remote Monitoring and Control Mechanism Using DNS for iot devices. The author has proposed a mechanism using DNS (Domain Name System where names or IDs of IoT devices are managed by DNS server and the monitoring and control are conducted by the collaboration of DNS name resolution, DNS dynamic update and DNS zone transfer. In the proposed mechanism, DNS is primarily used for name management of IoT devices, in addition that, DNS also contribute to providing secure and lightweight remote monitoring and control features using UDP, TSIG, zone transfer and dynamic update. Information of IoT devices is encrypted and only can be decrypted on authorized machines due to privacy protection.

Hokeun Kim and Edward A. Lee, et.al[7] has worked and presented an authentication and authorization for IOT. Access control is the process of determining whether an entity can access resources.Authorization also includes denying or canceling access, for someone or something malicious. Authentication is a process of identifying an entity which is a prerequisite for authorization. Passwords are the most common techniques to authenticate users. For additional security, we often use two-factor authentication such as phones, fingerprints etc.

S. Sridhar, Dr. S. Smys et.al [7] has discussed a framework for iot devices security. The main objective of the approach is to provide intelligent service by linking different platforms. Because of heterogeneous nature security issues like privacy and confidentiality arises. So an Intelligent Security Framework for IoT Devices is proposed. The proposed strategy contains light weight Asymmetric cryptography for anchoring the End-To-End gadgets which ensures the IoT benefit passage and the low power sensor hubs and (2) executes Lattice-based cryptography for anchoring the Broker gadgets/Gateway and the cloud administrations. The proposed convention utilizes the one of a Device ID of the sensors to create key match to build up shared confirmation among Devices and Services.

Shantanu Pal, Michael Hitchens, et.al[8] has proposed a Secure Access Control Architecture for the Internet of Things. The proposed approach uses secure access control architecture based on the interactions between things and service discovery in constrained networks. A dynamic policy management is applied for attributes in role membership assignments and permissions, effectively reducing the number of policies for granting a access to an IOT system.

Mihai Togan, Bogdan-Cosmin Chifor, et.al[9]has proposed an authentication service service for smart-home devices using a smart-phone as security anchor, QR codes and attribute based cryptography (ABC).in an IoT ecosystem some of the IoT devices and the cloud components are considered to be untrusted. So a privacy preserving attribute based access control protocol to handle the device authentication to the cloud service FIDO UAF protocol is used. Firstly, QR-based authentication service is used. The QR codes are used for the user credentials transfer between user mobile device and the smart home IoT device, in order to access an on-line service.

Maria Almulhim, Noor Zaman et.al [10] has put forwarded a lightweight authentication scheme for E-health applications, which verifies each IoT device and builds secure channels among the sensor nodes and Base Station (BS). Therefore, the scheme verifies each individual nodes and process the session key agreement among base station and sensor nodes within the time limitations. The scheme which is put forth is being assessed against the development of multiple events such as: Impersonation attacks, man in the middle attack and unknown key sharing attacks for IoT domain.In order to save the energy, arrangements should be made in advance depending on the group-based authentication model, in which the data present in the respective nodes is moved towards the group head that in turn, communicates with the base station. This node may be selected based on the distance in order to reduce the communication cost and to find a solution within a desired time limit.

AakankshaTewari, B. B. Gupta, et.al [11] has presented a robust anonymity preserving protocol for authenticating IOT devices. The proposed approach uses Pseudo random Number Generators is the process in which the numbers are generates randomly. A random number is being kept private and the curve point is calculated which is made public. The selected random number is verified and stored in the server’s database. The message is exchanged in the authentication phase and the calculations are done by the tag. The reader first sends a message and after the message is received the tag generates two random numbers.

Chan Hyeok Lee, Ki-HyungKim,et.al [12] has designed a system environment was being put forward with the help of IoT server platform, a system was designed in which we can share sensor data from device to application and transfer the data to a block chain server. In the block chain environment, Ethereum smart contract is used to increase the reliability and all the users can prove it by placing the power data on the block chain network. Smart contract was created with the Zero Knowledge Proof function, in which the quality of the block chains further increases in order to prevent the account information or data from being disclosed.

Juhi Bhatt, Anita Joshi, SunitaBisht, et.al[13] have described the hybrid solutions with new working techniques for securing the IoT communication. The main aspect is to provide security in the fields of authentication and data confidentiality. In existing methodology, using Radix-64 encryption is done to such an extent that finding out something new is done effectively and the protection is not that expected. In proposed methodology, using Radix-64 encryption is done we are using hash function in authentication to decode hash function. In the proposed methodology, the process of verifying the nodes and the information which is kept private is checked if the node is giving out some information the message fails then the authentication or information which is kept private is invoked by the sender.

Stephen Wilson, NourMoustafa, et.al[14] has proposed a novel digital identity stack to provide privacy for the data in IoT. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices

It consists of two phases: Setup phase and Authentication phase.

1. Setup phase: To start the setup phase, registration is requested along with its identity to the server. A server generates a challenge after receiving the request. After the challenge is being received the device takes out the output and sends it to the server. From now on the server generates a one-time alias identity key and a set of unique fake identity and synchronization key pairs. Finally, the server stores in its database.

2. Authentication Phase: This phase consists of the following steps:

Step 1: Request for Interaction

Step 2: Server Response

Step 3: Server Authentication

Step 4: Device Authentication

Kumar Sekhar Roy,Hemanta Kumar Kalita et.al[15] has proposed Authentication scheme that provides two types of authenticating primitives. Using BAN logic, they can prove the security of the authentication scheme. The scheme provides individual user, ensure the security of a communications and wrong password detections. Using a secure channel scheme must be transferred in some of the security primitives. A centralized control server is used for the flow of authentication data. A mutual authentication is established between all the entities

Trusit Shah, S. Venkatesan et.al [16] has addressed a new technique of authenticating IoT devices using the algorithm analysis and security. The algorithm is compared with Elliptic Curve Cryptography based encryption of public key and a simple 3-way authentication mechanism. ECC is used in IoT devices.

Muhammad Naveed Aman, SachinTaneja, et.al[17] has proposed a Token-Based Security for IoT. Before accessing a server on another IoT device, every IoT device must verify itself with an authorization server. The authorization server gives the permission to the IoT device with the security context which defines the scope and lifetime of the session. Hence we consider two phases among which the first phase obtains security process from an authorization server and the second phase enters a service. For each IoT device the authorization server starts with a single CRP. To obtain the initial CRP Time-based One-time Password algorithm can be used. The initial CRP gets exchanged with the server, when it is installed for the first time. Once the initial CRP is exchanged, the IoT device need not necessarily store the information and operator is not required in turn it can function independently.

Zahoor Ahmed Alizai, Noquia Fatima Tareen et.al [18] has presented an improved device authentication scheme for IoT. The first important thing is how efficient is the authentication scheme. The most important factor is multi-factor authentication which is efficient and secure and contains extra load on the device. In the TLS channel, public and private keys of both the server and device are used for authentication. A device performs a functional operation which acts as a second factor for authentication. Server is validated based on the performance of a functional operation.

IV. CONCLUSION

Internet of Things is emerging rapidly and helping to improve modern life by communicating and connecting with smart things. IoT is allowing for automation of all objects around us. IoT finds various applications in modern era like agriculture, defense, home automation, monitoring etc. In this paper we discussed about architecture of IoT and how the objects interact with user followed with a survey of existing approaches employed in securing IoT devices.

REFERENCES

[1] Chunye Hu1, Jie Zhang , Qiaoyan Wen, “AN IDENTITY-BASED PERSONAL LOCATIONSYSTEM WITH PROTECTED PRIVACY IN IOT”, Proceedings of IEEE IC-BNMT2011.

[2] Swati Kinikar Dr. Sujatha Terdal, “Implementation of Open Authentication Protocolfor IoT Based Application”, IEEE International Conference on Inventive Computation Technologies (ICICT) 2016.

[3] Shadi Janbabaei, Hossein Gharaee, Naser Mohammadzadeh, “Lightweight, Anonymous and Mutual Authenticationin IoT Infrastructure”, IEEE 8th International Symposium on Telecommunications (IST'2016), 2016.

[4] Hokeun Kim, Eunsuk Kang, Edward A Lee, David Broman, “A Toolkit for Construction of Authorization ServiceInfrastructure for the Internet of Things”, Proceedings of The 2nd ACM/IEEE International Conferenceon Internet-of-Things Design and Implementation, Pittsburgh, PA USA,April 2017.

[5] Yong Jin ,Masahiko Tomoishi,Nariyoshi Yamai, “A Secure and Lightweight IoT Device RemoteMonitoring and Control Mechanism Using DNS”, IEEE 41st Annual Computer Software and Applications Conference, 2017.

[6] Hokeun Kim and Edward A. Lee, “Authentication andAuthorization for theInternet of Things”,IT Professional Journal ,Volume: 19 , Issue: 5 , 2017 .

[7] S. Sridhar, Dr. S. Smys, “Intelligent Security Framework for IoT DevicesCryptography based End -To- End security Architecture”, International Conference on Inventive Systems and Control(ICISC-2017).

[8] Shantanu Pal, Michael Hitchens, Vijay Varadharajan," Towards A Secure Access Control Architecture forthe Internet of Things", IEEE 42nd Conference on Local Computer Networks, 2017.

[9] Mihai Togan, Bogdan-Cosmin Chifor, Ionuţ Florea, George Gugulea," A Smart-phone Based Privacy-PreservingSecurity Framework for IoT Devices", International Conference – 9th EditionElectronics, Computers and Artificial Intelligence29 June -01 July, 2017, Targoviste, ROMÂNIA.

[10] Maria Almulhim, Noor Zaman, "Proposing Secure and Lightweight AuthenticationScheme for IoT Based E-Health Applications", International Conference on Advanced Communications Technology(ICACT), 2018.

[11] Aakanksha Tewari, B. B. Gupta, "A Robust Anonymity Pr1e serving AuthenticationProtocol for IoT Devices", IEEE International Conference on Consumer Electronics (ICCE), 2018.

[12] Chan Hyeok Lee, Ki-Hyung Kim, "Implementation of IoT System using BlockChainwith Authentication and Data Protection", International Conference on Information Networking (ICOIN) 2018.

[13] Juhi Bhatt, Anita Joshi, Sunita Bisht, Kamlesh C. Purohit, "Hybrid Approach for Securing IoT Communication UsingAuthentication and Data Confidentiality", 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) 2017.

[14] Stephen Wilson, Nour Moustafa, Elena Sitnikova, "A Digital Identity Stack to Improve Privacy in the IoT ", IEEE 4th World Forum on Internet of Things (WF-IoT), 2018.

[15] Kumar Sekhar Roy,Hemanta Kumar Kalita, "A Survey on Authentication Schemes in IoT", IEEE International Conference on Information Technology, 2017.

[16] Trusit Shah, S. Venkatesan, "Authentication of IoT Device and IoT Server UsingSecure Vaults", 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12thIEEE International Conference On Big Data Science And Engineering, 2018.

[17] Muhammad Naveed Aman, Sachin Taneja," Token-Based Security for the Internet of ThingsWith Dynamic Energy-Quality Tradeoff", IEEE Internet ofThings Journal 2018.

[18] Zahoor Ahmed Alizai, Noquia Fatima Tareen, "Improved IoT Device Authentication Scheme UsingDevice Capability and Digital Signatures", International Conference on Applied and EngineeringMathematics,2018.