Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Secure Authentication and Security System for IoT Environment

Gagana M C [1], Chandana K J [2], Divyashree N [3], Mohammed Affan [4]
UG Students, dept. of CSE,
Vidyavardhaka College of Engineering.
Mysuru, India

Dr. Ravi Kumar V [5], Prof. Tanuja Kayarga [6]
UG Students, dept. of CSE,
Vidyavardhaka College of Engineering.
Mysuru, India

***Abstract*— In today's world many devices are connected via the internet. This provides any third person to intrude and control the IoT system. IoT is an emerging field, it involves devices which are interconnected through some network protocols. The major security issues of IoT are authentication, confidentiality and privacy. This paper gives the detailed technologies and techniques used to handle the security breach.**

Keywords—IoT, middleware, multi key authentication mechanism, CP- ABE, bilinear pairing, central attribute authority, AVISPA, REST API, RSA, AES, SHA-512, HIoTS, fog computing, DLTS.

I. INTRODUCTION

The Internet of Things (IoT) nowadays lacks security. As IoT is becoming our part of everyday routine, this security issue can become a greater threat. IoT applications include smart homes, responsive environments and many more, in some of these cases it is beyond the user's control. Devices with internet connections are always open to threats. Attacks on IoT or a website is always with a purpose and all these attacks are human-generated. The purpose of the attack varies dependingupon the intruder's target. IoT devices are operated by humans and intruder may want to gain access the confidential information by eavesdropping. IoT devices run on low power and a few computing resource capabilities. Considering all these limitations complex security protocols cannot be used.

An IoT middleware can be used as a security system. Figure 1 give us an idea about the implementation of the middleware in between the user and IoT device.

The IoT middleware is accessed and the keys inside the IoT device can be retrieved. Using these stolen keys, a duplicate IoT environment is created. Current single password-based mechanism, areless secure and are prone to attacks.

In this paper Section II shows the related works, Section III shows the literature survey. Section IV shows the comparative analysis of different authentication mechanisms and security systems for IoT environments. Section V is the conclusion of the paper

II. RELATED WORKS

Hittu Garg, Mayank Dave. [1] The author put forwards a model which is aimed to provide security and efficiency and reduces work load on the cloud by using middleware as an extra layer. AVISPA tool has been used to strengthen the proposed scheme.

Hittu Garg, Mayank Dave. [2] The solution proposed in this paper aims to provide an end-to-end security service to the middleware architecture and for the contributors who upload sensing data from IoT devices to cloud.

Leandro Loffi∗, Carla Merkle Westphall†, Lukas Derner Grudtner ¨, Carlos Becker Westphall [3] The proposed scheme is aimed to provide an authentication scheme which verifies mutually in an IoT environment applied with the help of Fog Computing.

Rohan A Nath S N Systems [4] The paper studies how to manage and secure the system traffic over internet by providing a pragmatic lightweight security scheme on transmission control protocol (TCP) network for remote monitoring system device over internet.

Trusit Shah, S. Venkatesan [5] This paper presents a design to provide a secure authentication mechanism between the server and the IoT device using multi-key based mutual authentication mechanism.

S. Sridhar, Dr. S. Smys [6] The proposed solution is aimed to provide a mutual and double authentication mechanism and an Intelligent Security Framework for IoT Devices.

Jin-Hee Han, JeongNyeo Kim [7] This paper presents a lightweight mutual authentication and dynamic session key scheme for IoT devices.

Shadi Janbabaei , Hossein Gharaee , Naser Mohammadzadeh [8] This paper presents a protocol between sensors in mobile mode and in the stationary mode which is mutually authenticated.

Thomas Kothmayr, Corinna Schmitt , Wen Hu , Michael Brunig and Georg Carle [9] This paper talks about a security scheme based on existing Internet standards and introduces a two way authentication protocol

Sheetal Kalra, Sandeep Sood [10] This paper presents a mutual authentication protocol for secured communication

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

between the cloud servers and the embedded devices based on ECC

III. LITERATURE SURVEY

In [1] the author proposes an IoT middleware which is an extra coat which links IoT devices and the cloud app and brings down work load on the cloud. For the users to safely access all the stored data from the cloud, the author uses Attribute-based encryption in the middleware.In ABE system, the data in the cloud can only be accessed by an eligible user only if he satisfies all thecondition set by the admin as an attribute. Example: If the admin sets ((X A Y) ∨ Z) as an attribute then, any user who is trying to access the cloud storage must have X and Y both the attributes or have only Z as an attribute. Only then the data is deciphered.

The Cipher text-policy attribute-based encryption scheme is one of the types of ABE. Registered userswill be allowed to access the cloud with security by using CP-ABE scheme. The computation overhead of bilinear pairing will be removed. A trusted Central Attribute Authority (CAA) will be introduced between the middleware and data owner which ensures that the user's information is kept safe and private from the outside world.

One central authority will be there in CP-ABE scheme, who distribute keys and this authority coordinates for avoiding collusion attack. Data owner, middleware, data users, and central attributeauthority are the entities which will be a part of access control scheme.The main advantage of using CP-ABE scheme is, only verified users can get the secret key according to the attribute they own. The CAA controls verified list of users with attributes, and CAA gets only the verified users from middleware. Thus, unauthorized users cannot go to CAA directly without going through the middleware. CAA will not allow decryption using attribute's secret key to the invalid user. Thus, this model is secured. AVISPA tool is introduced in addition to strengthen this proposed scheme.

In [2] the author proposes OAuth, an open authorization protocol with which the user can access the middleware with a username, password and token. In the first step, the device must register with the middleware and create an online file. If an IoT device sends a request for authentication, the gateway checks the device request by accessing the exposed REST API in the next step. Finally, the gateway sends the request access with its own to the exposed API credentials. Input parameters like secret key and the ID of gateway are transmitted with the request. Next, it is validated by the API, which authenticates and authorizes the request. As soon as the gateway is authorized, a form which is encrypted with details of the device is sent to the gateway as a response and after verification the device is assigned an access token by the gateway. Now real-time data will be exchanged between thedevice and the gateway.

In [3], the author proposes a new model to ensure the coherence of IoT contexts using Fog Computing into two processes: Hand Shaking and authorizing facts sections. During the handshake three things are analyzed to make sure Nonce, Challenge response and response time work. Existing procedures like SHA-512, AES and RSA have been repaired. Verification is carried out, especially during the authorization of the Authentication Factors proposed by the author has the same features as those of the TLS (Transport Layer Security) legal contract, but with something else relatedto its verification and its verification features. The results obtained from this project indicate that the authentication method model has been developed and validation is done using the AVISPA compliance testing tool, in an area which is memory restricted and is controlled by Fog Computing. Interms of cloud computing, there are route changes so it is more suitable in Mist Computing.

In [4], the author proposes embedded devices with remote sensing. IoT devices that are capable of remote sensing transfer the data in such a way that the intruder can easily access it by performing security attacks. Remote sensing technology is used in agriculture, medical, industrial, and many other fields. The improvement in the field of IoT has led to a revolution in the Remote Monitoring system. Figure 2 give us an idea of the architecture of RMS devices.

Remote Monitoring Network Architecture consists of three layers a) Sensing layer b) Presentation layer c) Network layer

The sensing layer is made up of a sensor network. The sensor network performs the task of sensing the raw data. The presentation layer will present all the collected data from the sensor network. The network layer transfers the data across the internet. Since these devices will be in continuous communication, a secured lightweight internet protocol between RMS IoT devices and the trusted party's server application.

In [5], the author proposes the most important part of secure IoT systems - Authentication between the IoT servers and the IoT devices should be mutual. Single-key or single password authentication is most commonly used and is most prone to attacks. This paper proposed an authentication based on multi-password or multi-key. Secure vault consists of the information which is shared among IoT devices and the IoT server. It is maintained a inside the vault as secret. The secure vault information is shared between the IoT device and the server. These contents will change after each successful communication session. The attacks on IoT devices may occur in single or multiple layers.

This paper proposes a mechanism for secure authentication which secures IoT devices and the server against side channel attacks. The passwords generated will change after every successful session.

This paper [6] focuses on the intelligent services of IoT. Internet of Things connects and links all the devices and provides us services, but it cannot provide us intelligent service. This is one of the drawbacks of IoT. IoT devices include less resource-constrained devices and different kinds of sensors. Hardware or software or network attacks is possible in these devices. To overcome the above-mentioned drawbacks a Security Framework is proposed. It consists of asymmetric cryptography which is light weighted for the security of end- to-end devices and lattice-based cryptography. This architecture uses the asymmetric

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

key for encryption to share session keys between the nodes. Later this session key will be used for transferring message. This protocol will help protect the system from different kinds of attacks, unique Device ID is used for generating the key. This key helps in establishing mutual authentication between the IoT devices. This paper first, proposes the framework for security purposes. Secondly, it gives an overview of the cryptography method. Secure communication can be provided using shared keys. Shared keys are confidentially exchanged by two parties. Public key is used for encrypting and private key for decrypting.

Implementation of cryptographic functions on constrained devices is complex. In this system we implement dual mutual authentication. For authentication we use light weight asymmetric key cryptography. The cloud service and the device will be mutually authenticated using digital signature which is encrypted using public key

In [7], the author uses block cipher algorithm for mutual authentication and dynamic session key generation. It uses 128-bit pre-shared secret key, two 64-bit random variables and identification information of devices.In order to verify whether the proposed mutual authentication mechanism is loaded in IOT device MS500 board and RIOT OS are used, for reference AES cryptographic library and TRNG (True Random Number Generator) also are utilized. The below figure shows the lightweight mutual authentication mechanism test results on MS500 board and RIOT OS based development environment

To guarantee the soundness and confidentiality of message transmitted between devices, base64 encoding function and also encryption function using dynamic session key are used while sending a message. Similarly, when receiving a message base64 decoding functions and decryption function using dynamic session key is also used.

In [8], the author proposes anonymous light-weight validation for IOT devices. The most critical security requirement in preserving privacy is anonymity. In this paper the author has introduced a distributed architecture of IoT. Two sensors designed and analyzed in an IoT environment using a mutual authentication protocol. The proposed protocol is unknown and unmanageable. This model consists of three steps: a registration, validation and authentication in different servers of HloT. This scheme is not more lightweight when compared to other scheme but has features like key agreement which is additional and is considering sensor validation in mobile and stationary modes. The sensorswill have any location restriction.

In [9] the author introduces a security scheme based on two-way authentication based on existing Internet standards. This scheme is introduced on the basis of DTLS protocol. The security scheme in this paper is based on public-key cryptography (RSA). There are three design decisions in DLTS – Implementing design based on standards: Where the uptake of technologies is motivated by standardization. Security of end-to-end devices is focused on application layer: Security is provided even if the infrastructure is not fully under the user's control. Transport protocols: Protocol like TCPwhich is reliable has advantage over unreliable protocol like UDP.

The evaluation made on IoT systems proves that the proposed architecture assures integrity, authenticity and confidentiality. This architecture is feasible due to memory overhead and end-to-endlatency.

In [10], the author talks about an embedded system which is a combination of a computer processor, computer memory, and input/output peripheral device that has a dedicated function within a larger mechanical or electrical system. Embedded devices performing single function can be called smart systems. All the organizations nowadays are collaborating their embedded systems with the cloud. Cloud computing is one of the most widely used and most popular technology. It has elasticity which is dynamic and plenty of resources. Cloud based technology will have both software and hardware which the data centers provide. The consumer must only pay for the resources which is been used. Thisis beneficial for internet-connected devices. However, by integrating the embedded devices and the cloud servers there might arise some security issues. A secure ECC (Elliptic Curve Cryptography) is proposed in this paper. This protocol helps in having secure communications. This protocol can be formally verified using the AVISPA tool. This helps in detecting the possible intruder. ECC protocol has a registration, pre-computation and login phase. In the registration phase, the device will registerin the cloud server. The server creates and store cookies on the device. Whenever connection is required between the device and the server, a login request will be sent. Finally, the cloud server and the embedded device will perform authentication by using the necessary parameters of ECC.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

IV. COMPARISON ANALYSIS OF DIFFERENT AUTHENTICATION MECHANISM AND SECURITY SYSTEM FOR IOT ENVIRONMENT

Sl no	Title of the paper	Objective	Methodology	Result	Drawbacks
[1]	"Securing User Access at IOT Middleware Using Attribute Based Access Control"	This scheme provides security and efficiency for the users to access the data on the cloud while reducing load on middleware. Attribute-based encryption (ABE) is used.	Cipher text policy-attribute based encryption	It gives privacy and security for the data on the cloud and only users who possess certain attributes are allowed to fetch data from the cloud.	Data security is based on data attributes and it's not independent of user's information. If the attributes of the user is modified then algorithm results invaliddata.
[2]	"Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware"	Provides an end-to-end security service through a middleware for the users who upload confidential data from IoT devices to cloud.	OAuth- An open authorization protocol is used at middleware or authentication. Data exchange and communication is done through REST API.	Middleware exposes device information through REST API and details are hidden and acts as a connection between the user and sensor data.	OAuth protocol at middleware uses only username, password, and tokens for authentication hence chances of data breach at middleware is high.
[3]	"Mutual Authentication for IoT in the Context of Fog Computing"	Designing an authentication model which jointly verifies both the devices in an IoT environment, put in factors of fog computing.	The proposed solution has characteristics sameas that of Transport Layer Security (TLS) handshake, but has a number of specifics related to mutual authentication and its authentication elements.	The proposed model put in factors of fog computing using response time and ad-hoc verification along with a simple "challenge-response" function which has an average of 24.03 ms for mutual authentication.	IoT devices can join or leave the networkat anytime and anywhere. These temporal and spatial devices make the network topology dynamic. Therefore, the current security of the network does not deal with this sudden type of topological changes, and working with confined devices which have many bugs due to memory and processing.
[4]	"Objective Secured TCP Socket for remote monitoring IOT devices"	Developing a secured lightweight internet protocol between RMS IOT devices and trusted third party's server application	The proposed scheme involves minimum handshaking to establish a secure session between application server and the device	Object Secured TCP, a light weighted and minimum handshaking security scheme	IOT RMS devices using TCP requireslong connection which might lead to attacks. Physical damage, hardware failure arethe other challenges faced
[5]	"Authentication ofIoT Device and IoT Server Using Secure Vaults"	To create a secure protocol for authentication between IOT device and the server.	Multi-key authentication mechanism. The unused authentication keys cannot be accessed even if the secret key is retrieved successfully.	The algorithm is secure against side channel attacks. After every successful session the set of passwords are changed.	The secure vault provides secure keyduring initial communication and authentication but problem with authentication may occur The Iot devices at the perception layer maybe prone to physical attacks
[6]	"Intelligent Security Framework for IoT Devices"	To develop an intelligent security framework.	Asymmetric Key Cryptography and Lattice-based cryptography.	By eliminating fault and fake packets using Mutual and double authentication schemes we can reduce traffic.	In IoT devices like wireless sensors which are in public areas will not have any protection. This makes the devices vulnerable to physical attacks and will be difficult to manage
[7]	"A Lightweight Authentication Mechanism between IoT Devices"	The main objective here is to develop a lightweight utual authentication and dynamic session key scheme for IoT devices.	ECB and CTR modeof block cipher algorithm for data encryption. ECB and CCM mode of block cipher for data encryption with data integrity.	A lightweight mutual authentication method between IoT devices which helps in access control and security policy setting.	Encryption is slow because, entire blockmust be accumulated before encryption/decryption to begin. An error in any one symbol corrupts theentire block.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

[8]	"Lightweight, Anonymous and Mutual Authentication in IoT Infrastructure"	The main objective here is to develop a protocol which is lightweight for mutually authenticating two sensors in stationary and mobile mode in an IoT environment.	It consists of twophases: [1] Registration phase. [2] Authentication phase	This protocol guarantees certain privacy and security such as confidentiality, inactivity, including key agreement and looks for sensor verification on both static and mobile modes.	The proposed model is not more lightweight when compared with other protocols of similar type. But only advantage is that it adds some extra characteristics like key agreement and both in stationary and mobile modes sensor authentication is done.
[9]	"A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication"	The main objective is to design a double way authentication security for IOT especially the Datagram Transport Layer Security (DTLS) protocol.	RSA algorithm which is a public key cryptography and it works on top of standard low power communication stacks.	Two-way authentications using standard security architecture is introduced for the IoT environment. Authenticated uses DTLS handshake.	Multicast communications is notsupported DTLS protocol. Exhaustion attack of the resources on the battery powered devices even with stateless cookie mechanism can be caused by DTLS handshake protocol.
[10]	"Secure authentication scheme for IoT and cloud servers"	The main objective is to design a mutual authentication protocol based on ECC for secure communication between the embedded device and cloud servers using HTTP cookies.	ECC based algorithms which uses small key sizes and efficient in computations.	This protocol is secureand robust against all the security threats. AVISPA tool performs automatic verification	It is difficult to implement ECC algorithm and is more prone to errors which reduces the security of the algorithm

V. CONCLUSION

Based on the above literature survey and current state of art on threats and security it has been found that there is a scope to work on this domain. Our focus is to develop a middleware between user and IoT Environment to ensure users are connected to IoT environment only upon multiple authentications that is even if the attacker successfully retrieves the secret key but fails to access the authentication keys which are unused and hence security is ensured to the authentication system. Since the values of keys changes over time any possible attacks can be prevented. Apart from this a secured channel required for the user and IoT device to communicate without any data breach in the middle and also log all the data into the ledger using block chain technology for any future validations.

REFERENCES

[1] H. Garg and M. Dave ,"Securing User at IoT Middleware Using Attribute Based Access Control," 2019 10th Internaltional Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6, doi:10.1109/ICCCNT45670.2019.8944879

[2] H. Garg and M. Dave, "Securing User Access at IoT Middleware Using Attribute Based Access Control," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944879.

[3] L. Loffi, C. M. Westphall, L. D. Grüdtner and C. B. Westphall, "Mutual Authentication for IoT in the Context of Fog Computing," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 2019, pp. 367-374, doi: 10.1109/COMSNETS.2019.8711402.

[4] R. A. Nathi and D. Sutar, "Object Secured TCP Socket for Remote Monitoring IoT Devices," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-5, doi: 10.1109/ICCCNT45670.2019.8944566.

[5] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00117.

[6] J. Han and J. Kim, "A lightweight authentication mechanism between IoT devices," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 1153-1155, doi: 10.1109/ICTC.2017.8190883.

[7] S. Janbabaei, H. Gharaee and N. Mohammadzadeh, "Lightweight, anonymous and mutual authentication in IoT infrastructure," 2016 8th International Symposium on Telecommunications (IST), Tehran, 2016, pp. 162-166, doi: 10.1109/ISTEL.2016.7881802.

[8] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G.Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," 37th Annual IEEE Conference on Local Computer Networks - Workshops, Clearwater, FL, 2012, pp. 956-963, doi: 10.1109/LCNW.2012.6424088.

[9] Karla, S.,& Sood S K "Secure authentication scheme for IoT and cloud servers" 2015,IEEE Conference.