I J C T A, 9(39) 2016, pp. 335-339

A Survey on IoT Authentication Schemes

Valmiki Siddhartha[1], Gurjot Singh Gaba[2], Rajan Miglani[3] and Sandeep Kumar Arora[4*]

ABSTRACT

Internet of Things (IoT) is one of the emerging technologies in IT. IoT is an interconnection of devices and these devices can be accessed and controlled from anywhere in the world with the help of Internet. It indicates a direct integration of computing systems with the computing world. IoT facilitate a lot of unimaginable services and applications which may carry precious data. There originates a requirement to secure IoT from threats. The authentication is a challenging task due to heterogeneity in devices that are interconnected in IoT. Authentication allows user to communicate with the device in a secured manner. In this paper, we present various authentication techniques that are proposed in the past to provide security in the IoT along with the performance analysis of the techniques against attacks.

Keywords: Internet of Things, Authentication, Protocol, Security, Attacks.

I. INTRODUCTION

Internet of things (IoT) is one of the latest emerging technologies in the IT. IoT is an interconnection of different physical objects that are communicating to each other through the internet. As there is a direct interface to the computing world, we need to provide security to the network from unauthorized users. IoT undergo several threats that can make irreversible damage to the IoT environment, so security and privacy mechanism should be used to prevent from this damage. IoT authentication schemes are designed to provide mutual authentication between user and the device in order to prevent the unauthorized user from accessing the network. Even biometric authentication can be used as a method to authenticate an individual by processing the face texture, iris, and fingerprints [3]. It uses the individuality as an authentication token and allows communication between user and device. In [4], the author used OAuth protocol which allows users to access the confined resources without providing their credentials. Table 1 & Figure 1 depict the OAuth protocol working where the user will initially visit the client application, where request will be directed to service provider. When service provider grant access to the client, the client will get authorization code, which in turn, can be used to request the service provider for access token. Once client gets access token, the client can access all the resources affiliated to him.

Table I
Dialogue Exchange

1	User opens the client application
2	User is redirected to service provider
3	User initiates the authentication process
4	Service Provider sends an authorization code for entity verification
5	Client uses the authorization code and client ID to request service provider for access token
6	After verifying client ID and authorization code, service provider grants the access to the client
7	Client uses this access token to access the resources of the user by sending request to service provider

[1,2,3,4] Discipline of Electronics and Communication Engineering, Lovely Professional University, Phagwara, Punjab, India - 144411, *E-mail: [1]valmikisiddhartha@gmail.com, [2]er.gurjotgaba@gmail.com, rajan.16957@lpu.co.in*

[*]Corresponding Author - [4]sandeep.16930@lpu.co.in[*]

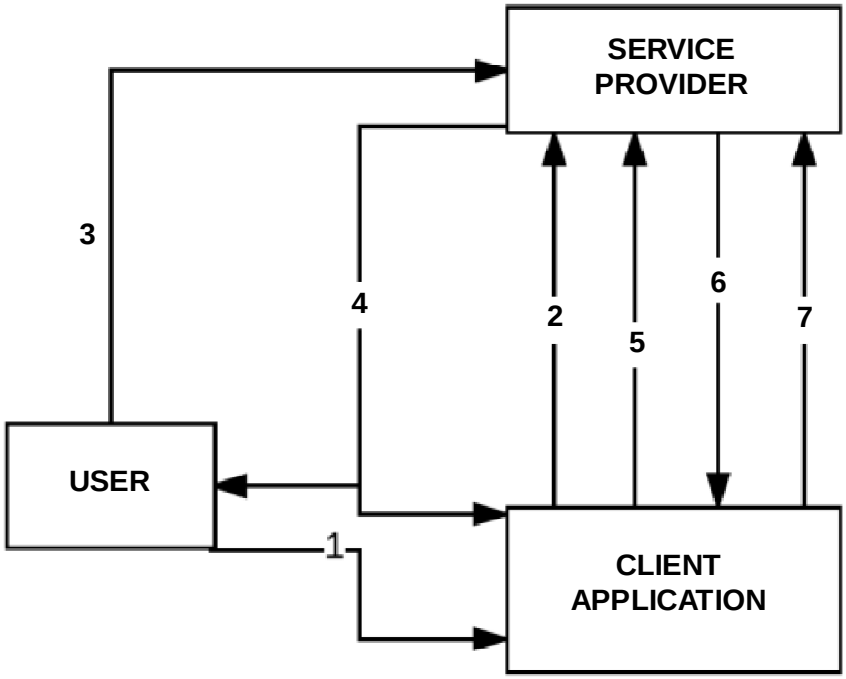

Figure 1: Dialogue Exchange: Standard OAuth Protocol

II. RELATED WORK

IoT authentication provides security from threats and attacks. The authors in the past discussed an approach of authentication using an identity-based scheme [1]. The proposed scheme is meant to address the heterogeneity in the internet of things by managing all the security parameters with a Software Defined Networking (SDN) controller. Heterogeneity refers to the large amount of 'IoT Big Data' which differs in attributes. The fact that IoT networks are interconnection of networks communicating through different networking protocols which result in heterogeneity in the form and amount of data. The communication between different nodes will represent a fog distributed environment; therefore a gateway is required to support the heterogeneity and to ease the authentication. SDN controller is a centralized controller which manages and monitors the network elements and their functions, even gateways are managed and authenticated by it. The advantage of SDN controller is, it reduces the management complexities that are present in the IoT and it can detect any misbehavior in the network.

The proposed authentication scheme is based on the assumption that the entire objects can be configured with IPv6 addresses. The proposed architecture contains SDN controller which is responsible for providing security and contains full knowledge of the different IoT domains in the surroundings. The authentication between things is provided by means of exchanging security keys. The key establishment method uses Elliptic Curve Cryptography (ECC). The proposed scheme constitutes of three phases for providing authentication such as Gateway public key certification, Thing registration, followed by Authentication phase. Therefore, this scheme is considered to be safe against man-in-the-middle, replay, and masquerade attacks.

A light-weight Radio Frequency Identification (RFID) mutual authentication protocol with a cache in the reader (LRMAPC) is proposed whose main purpose is to reduce the computational complexity [2]. It is achieved by storing the recently visited key tags information in the cache memory and these tags are authenticated directly by the reader thereby reducing the transmission cost. Internet of Things (IoT) is an interconnection of large number of devices like sensors and actuators. Radio Frequency Identification (RFID) is an information sensing device and it plays an important role in the IoT. Since the storage space and computational capabilities are limited in the RFID system, it cannot use high power consumption

security protocols. The author proposed secure mutual authentication scheme using hash function in order to address the security issues of the low-cost RFID system. The proposed scheme provides secure against Denial of service, Tracking, Spoofing, Replaying, and Eaves dropping.

The authors of [3] built their authentication scheme based on the transparent authentication strategy. They proposed a transparent authentication scheme with adaptive biometric features for IoT networks. The scheme will analyse the individual's foot pressure and extract the unique biometric features for continual user identification and verification. The machine learning technique i.e. support vector machine with Gaussian radial basis function (SVM-GF) is used for extracting user bio-features as authentication tokens for performing real-time entity verification transparently.

A secure authentication mechanism which protects IoT networks from unauthenticated users using Open standard authorization (OAuth) 2.0 protocol was evolved in 2015 [4]. The authors proposed a two-step process; the authorization process uses OAuth 2.0 protocol where user requests access to security manager through service provider. In authentication process, security manager compares the user ID obtained from the service provider through access token with its local database, if in turn it matches, and then only user is allowed to access the IoT network. Standard OAuth protocol provides access to all the users requesting from specified service provider but the proposed approach avoids this situation by allowing only authenticated user to access the network. OAuth protocol is subjected to impersonation and replay attack but OAuth 2.0 protocol provides security against these attacks. The main advantage of this approach is that it reduces the burden for users from registering to multiple networks and it saves the effort of maintaining a secure database in the IoT networks.

A novel authentication frame work [5] to make use of device specification information, called finger prints is used to evade unauthorised access. Finger prints are used to authenticate objects in the IoT. The author differentiated the security attacks and normal changes in finger prints, in order to effectively track the effects of physical environment on objects via a transfer learning tool. Due to the heterogeneity between objects, they can be easily authenticated by using device finger prints. The author divided the object set into multiple hierarchies based on geographical location and the types of finger print features because every object contains its own finger prints, geographic location and physical state. The author assumed that finger prints collected from same object will follow a certain distribution and the collected finger prints as a set of distributions. The authors used transfer learning approach to authenticate objects of different feature spaces and to prevent the emulation attack. The author implemented two-fold approach to authenticate an object. Firstly, a generative based approach is used i.e. Infinite Gaussian Mixture Model (IGMM) assuming that each object finger prints follow a multivariate Gaussian distribution. Secondly, these finger prints will be verified by comparing the clustering results from the IGMM with the expected cluster shape for the object. To detect the environmental effects on IoT, transfer learning approach is being used. Thus, by combining the knowledge from different finger print features we can track the environmental effects on IoT objects. This technique is significant as the device finger printing techniques along with transfer learning approach can detect the presence of emulation attacks.

An asymmetric mutual authentication scheme is proposed [6] between the platform and terminal node by integrating the secure hash algorithm (SHA), feature extraction and elliptic curve cryptography. Due to the combined use of hash algorithm and feature extraction, this scheme can prevent the collision attack and it can reduce the consumption of resources. The author explained the mutual authentication scheme in three phases; the first phase is initialization phase. The second phase is verification; here certificates are verified securely. The third phase is the mutual authentication where asymmetric scheme is adopted for platform and terminal node. This scheme stores the residual private key in the terminal node leaving it to the platform node to decide what could be the other part of the private key. It uses the random method or elliptic projection to generate the private key and then it sends this key to the terminal node. After receiving,

the terminal node computes the private key. This key agreement saves the memory space. The security is provided to the system by elliptic curve discrete logarithm problem.

In [7] the authors proposed a dynamic and energy aware authentication scheme for the Internet of Things (DAoT). This authentication mechanism uses the feedback control scheme to dynamically select an energy efficient authentication policy. Though existing authentication policies were successful in preventing man in the middle attack but those authentication schemes did not considered the energy issues and resource constraints of the devices. To encounter these issues, the authors suggested an IoT-accommodating authentication policy. Design goals associated with DAoT are adaptive and energy-aware authentication. By using this authentication scheme, IoT devices with fewer resources can be interconnected safely in the network.

III. RESULTS & DISCUSSIONS

Performance of the authentication techniques depends upon the strategy used for authentication and resistance of the technique against attacks. Table 2 summarizes the various strategies used for IoT authentication in the last decade. Among these, some approaches are reliable and provide better security. It is observed that all the techniques differ in strategies used for Authentication.

Table 2
IoT Authentication Schemes

Authentication Schemes	*Mechanism used for Authentication*
[1]	Software Defined Networking, Elliptic Curve Cryptography.
[2]	Lightweight RFID Mutual Authentication Protocol, Hash function.
[3]	Transparent Authentication scheme, Machine Learning technique.
[4]	OAuth 2.0 protocol
[5]	Transfer Learning tool, Finger print technique.
[6]	Asymmetry mutual authentication scheme, Secure Hash Algorithm, Feature Extraction, Elliptic Curve Cryptography.
[7]	Dynamic and Energy-aware Authentication mechanism, Feedback control Scheme.

The efficiency of the technique and its applicability depends upon the resistance of the authentication scheme against attacks. Table 3 summarizes the various attacks that are prevented by the corresponding Authentication schemes, hence reporting the strength of traditional schemes.

IV. Conclusion

IoT is a network of things interconnected through internet. Every physical object connected to the internet is under threat of cyber crime. To avoid unauthorised users gaining access and to prevent disclosure of information to malicious users, various techniques of authentication have been evolved in the last decade. These techniques use different principles for achieving authentication. It is quite noticeable that different techniques are subjected to different sort of attacks. Hence, there is a requirement of a technique which consumes less power, less bandwidth, less overhead and has strong resistance against attacks.

Table 3
Attacks

Authentication Schemes	*Prevention Against Attacks*
[1]	Masquerade, Man-In-The-Middle, Replay.
[2]	Denial of Service, Tracking, Spoofing, Replay, Eaves drop.
[3]	Not Specified
[4]	Impersonation, Replay.
[5]	Emulation
[6]	Collision, Replay, Man-In-The-Middle.
[7]	Man-In-The-Middle

REFERENCES

[1] Ola Salman, Sarah Abdullah, Imad H. Elhajj, Ali Chehab and Ayman Kayssi. "Identity-Based Authentication Scheme for the Internet of Things," IEEE Symposium on Computers and Communication (ISCC), Beirut, Lebanon, pp.1109-1111, 2016.

[2] Kai Fan, Chen Liang, Hui Li and Yintang Yang. "LRMAPC: A lightweight RFID mutual authentication protocol with cache in the reader for IoT," IEEE International Conference on Computer and Information Technology (ICCIT), China, pp.276-280, 2014.

[3] Kuo-Hui YEH, Chunhua SU, Chien-Lung HSU, Wayne CHIU and Yu-Fan HSUEH. "Transparent Authentication Scheme with Adaptive Biometric Features for IoT Networks," IEEE 5th Global Conference on Consumer Electronics (GCCE), pp.1-2, 2016.

[4] Shamini Emerson, Young-Kyu Choi, Dong-Yeop Hwang, Kang-Seok Kim and Ki-Hyung Kim. "An OAuth based Authentication Mechanism for IoT Networks," IEEE International Conference on Information and Communication Technology Convergence (ICTC), pp.1072-1074, 2015.

[5] Yaman Sharaf-Dabbagh and Walid Saad. "On the Authentication of Devices in the Internet of Things," IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Blacksburg, VA, USA, pp.1-3, 2016.

[6] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long, Ting Hu. "A Novel Mutual Authentication Scheme for Internet of Things," Proceedings of 2011 International Conference on Modelling, Identification and Control, Shanghai, China, June 26-29, pp.563-566, 2011.

[7] Young-Pil Kim, Seehwan Yoo and Chuck Yoo. "DAoT: Dynamic and Energy-aware Authentication for Smart Home Appliances in Internet of Things," IEEE International Conference on Consumer Electronics (ICCE), pp.196-197, 2015.