International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)

An Extensive Study on Authentication and Authorization of IOT Devices

Bharath Alli
Project Lead, Ford, Detroit, Michigan, India

Article Info
Volume 7, Issue 6
Page Number : 443-452

Publication Issue :
November-December-2021

Article History
Accepted : 15 Dec 2021
Published : 30 Dec 2021

ABSTRACT

The rapid proliferation of the Internet of Things (IoT) into diverse application areas such as building and home automation, smart transportation systems, wearable technologies for healthcare, industrial process control and infrastructure monitoring and control is changing the fundamental way in which the physical world is perceived and managed. It is estimated that there will be about 30 billion IoT devices by 2020. Most of these IoT devices are expected to be of low-cost and wireless communication technology based, with limited capabilities in terms of computation and storage. As IoT systems are increasingly being entrusted with sensing and managing highly complex eco-systems, questions about the security and reliability of the data being transmitted to and from the IoT devices are quickly becoming a major concern.

Index Terms : Internet of Things, authentication, authorization

I. INTRODUCTION

Privacy and security are among the significant challenges of the Internet of Things (IoT). Improper device updates, lack of e*ffi*cient and robust security protocols, user unawareness, and famous active device monitoring are among the challenges that IoT is facing. In this work, we are exploring the background of IoT systems and security measures, and identifying (a) di*ff*erent security and privacy issues, (b) approaches used to secure the components of IoT-based environments and systems, (c) existing security solutions, and (d) the best privacy models necessary and suitable for di*ff*erent layers of IoT driven applications. In this work, we proposed a new IoT layered model: generic and stretched with the privacy and security components and layers identification. The proposed cloud/edge supported IoT system is implemented and evaluated. The lower layer represented by the IoT nodes generated from the Amazon Web Service (AWS) as Virtual Machines. The middle layer (edge) implemented as a Raspberry Pi 4 hardware kit with support of the Greengrass Edge Environment in AWS. We used the cloud-enabled IoT environment in AWS to implement the top layer (the cloud). The security protocols and critical management sessions were between each of these layers to ensure the privacy of the users' information. We implemented security certificates to allow data transfer between the layers of the proposed cloud/edge enabled IoT model. Not only is the proposed system model eliminating possible security vulnerabilities, but it also can be used along with the best security techniques to countermeasure the cybersecurity threats facing each one of the layers; cloud, edge, and IoT.

The Internet of Things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless. The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development. IoT introduced the hyperconnectivity concept, which means organizations and individuals can communicate with each other from remote locations effortlessly. Kevin Ashton invented the term 'IoT' in the year 1999 for promoting the Radio Frequency Identification (RFID) concept, which includes embedded sensors and actuators. However, the original idea was introduced in the 1960s. During that period, the idea was called pervasive computing or embedded Internet. Ashton presented the IoT concept to improve supply chain activities. However, diverse functionalities of IoT has helped it to gain strong popularity in the summer of 2010. The Chinese government gave strategic priority on IoT by introducing a five-year plan. About 26.66 billion IoT devices exist in the current world [1]. The mass explosion started in 2011 with the introduction of home automation, wearable devices, and smart energy meters. The rapid explosion of IoT has benefitted organizations and in various ways improved market research and business strategies. Similarly, IoT has improved the lifestyle of individuals by introducing automated services. However, such an uncontrolled explosion has increased privacy and security challenges.

The unconscious use, not changing passwords, and the lack of device updates have increased cybersecurity risks and access to malicious applications to the IoT systems' sensitive data. Such inappropriate security practices increase the chances of a data breach and other threats. Most of the security professionals consider IoT as the vulnerable point for cyber attacks due to weak security protocols and policies. Even though several security mechanisms were developed to protect IoT devices from cyber attacks, security guidelines are not appropriately documented [2]. Thereby, end-users could not utilize protective measures to avert data attacks. Hackers developed different kinds of malware to infect the IoT devices since the eve of 2008. They designed various phishing techniques to provoke the employees or individuals to share sensitive data. Therefore, corporate workstations and personal devices often face privacy violations due to high-profile attacks. If device manufacturers and security experts assess the cyber threats accurately, they can develop an efficient protective mechanism to prevent or neutralize cyber threats.

IoT enabled devices have been used in industrial applications and for multiple business purposes. The apps help these businesses to attain a competitive edge over their competitors. However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services. It is essential to have professionals to overcome these threat concerns and develop comprehensive security measures and policies to protect their business assets and ensure services continuity and stability. For example, smart kitchen home IoT enabled appliances connected to the local network can be a source of the breach for hackers to get access to the business and/or personally sensitive data or to manipulate and interrupt the business workflow.

Every day new technologies emerge, or changes are made to existing ones. Consider the latest advances in the 5G network, for example. 5G is expected to play an essential role in the IoT systems and applications. It is getting the researchers' attention and curiosity about the possible security and privacy risks, with its high frequency and bandwidth. Yet, the short wavelength imposes a change in the infrastructure, hence the need for more base stations to cover the same area covered by other wireless technology. This

new structure imposes more threats, such as fake base stations. It is essential to understand the security risks and potential solutions.

In this work, we aim to provide an overview of the IoT applications, benefits, and potential risks. Additionally, to build a framework to study and further develop best security practices by either implementing and analyzing current existing schemes or developing new ones. Based on the findings, we provide recommendations to avoid such risks and to remedy the possible security vulnerabilities. This work will guide regulatory agencies to continue enforcing policies, educating end-users and entities, and stakeholders involved in IoT to develop and apply more appropriate security and privacy measures.

We built our model using Amazon Web Service (AWS) as proof of concept, which later translated to actual physical systems of sensors nodes mimicking general IoT structure. By making the system, we can deploy and study di*ff*erent security approaches by building real sceneries and benchmarks.

We adopted a narrative review methodology to explore the history and background of the IoT systems, their security and privacy issues, and the corresponding countermeasures. We proposed our own view of the generic and stretched IoT model and its privacy and security concerns. We built and studied a cloud/edge supported IoT model consisted of a virtual machine (sensors), and edge node (Raspberry Pi), and cloud services (AWS). This setup was designed to evaluate the model we proposed in the following sections in this paper. Our work does not provide details on the di*ff*erent IoT applications (smart health, smart cities, supply chain, transportations, etc.); their features, advantages, and challenges, or the possible security risks or threats among these applications. The point of computing devices having such potentially catastrophic vulnerabilities is not merely academic. It can happen—unfortunately too easily in practice. There have been numerous demonstrations of attackers being easily able to inject malicious code directly into wearable devices by using programming interface and then acquire sensitive data of users. There have been demonstrated attacks on implantable medical devices, such as implantable cardioverter defibrillator (ICD), which seriously threaten the patient's life safety. Attacks in industry and urban infrastructure also show an increasing trend. In the field of automotive embedded systems, more and more electronic devices and embedded devices are used in many high-end automobiles. The attacker can gain control of the car due to the lack of security protection in these devices, such as electronic control unit (ECU) attack. This would have a serious security threat to the driver. Attacks on urban infrastructure can affect the social order, such as attacks on transportation and logistics.

In this paper, we consider the spectrum of challenges, approaches, and practice in IoT security. IoT security is unique in many respects and introduces diverse challenges different from those in security assurance of other computing devices such as desktops, laptops, servers, or even mobile devices. We develop two taxonomies of security attacks specifically for the IoT regime. The first taxonomy introduces attacks on the four-layer architecture of IoT (perception layer, network layer, middleware layer, application layer). Based on this taxonomy, we systematically analyze the security threats and privacy issues on every layer of IoT. The attacks can occur in each layer, and we need to provide protection for the entire IoT structure, not just for the specific technology. Another taxonomy of IoT security and vulnerabilities is based on different application scenarios. This provides an analytical basis for the protection of different IoT applications.

II. LITERATURE REVIEW

The author in [3] stated that Besides prospective security layout lacks, the sizable rise in the amount in addition to characteristics of IoT resources could bring up the possibilities of the strike. When paired

in addition to the highly connected quality of IoT devices, every improperly safeguarded device that is hooked up online likely affects the security and likewise durability of the Internet around the world, not just in your area. As an example, a prone refrigerator or even television in the USA that is tainted along with malware could send bunches of harmful spam e-mails to receivers globally utilizing the proprietor's house Wi-Fi Internet. There are potential solutions that can help the individual to implement various security measures that can help to secure their IoT devices. According to [6], various privacy threats have emerged in the present time, and they can penetrate IoT Technologies and their integrated network. It is not easy to manage the security of IoT devices in businesses and organizations. The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Tra*ffi*c interceptors and analyzers help identify and investigate various cyber threats.

There are various studies as well as services that have been conducted on the current trends in IoT security [7]. Multiple services have presented some of the challenges or attack vectors to various IoT devices and their guards. Various simulation tools, modelers, and the availability of numerous platforms that can confirm this security protocol can also help in producing the protocol related to novel IoT security. It is fair to say that there has been rapid progress in terms of research related to IoT security and various simulation tools as well as modelers have supported this research. If the IoT devices failed, then the issues will be severe.

The author Mr. Vivek Thoutam[3] believe that IoT units tend to comparison coming from conventional pc units and likewise computing devices in important manner ins which challenge security:Tons of Internet of Things resources, consisting of sensing units alongwith consumer items, are established to be released at a sizable variation that is investments of measurement beyond that of traditional Internet-connected tools.

The authors in [8] believe that, despite the enormous benefits the users are getting from the Internet of Things, there are challenges that come along with it that need to be looked at. Cybersecurity and privacy risks are the primary concerns that have been cited. These two are posing a massive predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet, requiring novel security solutions. On the other hand, it is important to emphasize the standards and basic principles of the IoT Cyber Security Framework when it comes to implementing the IoT security system. According to [9], one of the most important measures to consider is the termination of a contract consisting of di*ff*erent devices with di*ff*erent communication protocols. The di*ff*erence in protocols hinder separate service contracts from implementation and are fundamental elements that must be present in the cybersecurity structure of every Internet of Things. He demonstrated that to ensure the reliability of the IoT framework in the cybersecurity arena, some small steps need to be taken to help mitigate the challenges of IoT cybersecurity. In addition, the authors in [9] showed that scalability is also an essential measure of the success of the cybersecurity Internet of Things framework. Analysts said the IoT environment needs to be scalable enough to handle a billion Internet-related and cybersecurity challenges. In addition, the magazine showed that the IoT cybersecurity environment should also support testability, such as integration testing, component testing, system testing, and compliance testing, e*ff*ectively reducing challenges and risks. In

the same context, the authors in [10] described some of the current IoT cybersecurity solutions.

Some basic security measures are implemented by the supplier, and state that it is not profitable for the supplier to produce high-quality solutions. In the case of cybersecurity of the Internet of Things, companies are unlikely to develop the right solution.

III. ATTACKS AND COUNTER MEASURES

Security is defined as a process to protect a resource against physical damage, unauthorized access, or theft, by maintaining a high confidentiality and integrity of the asset's information and making information about that object available whenever needed. The IoT security is the area of endeavour concerned with safeguarding connected devices and networks in the Internet of Things environment. IoT enables to improve several applications in various fields, such as, smart cities, smart homes, healthcare, smarts grids, as well as other industrial applications. However, introducing constrained IoT devices and IoT technologies in such sensitive applications leads to new security challenges.

IoT is relying on connectivity of myriads of devices for its operation. Hence, the possibility of being exposed to a security attack is most probable. In IT, an attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to an asset. For example, cryptographic security protocols are a key component in providing security services for communication over networks [10]. These services include data confidentiality, message integrity, authentication, availability, nonrepudiation, privacy [3]. The proof of a protocol flaw is commonly known as an "attack" on a protocol and it is generally regarded as a sequence of actions performed by a dishonest principal, by means of any hardware or software tool, in order to subvert the protocol security goals. An IoT attack is not peculiar from an assault against an IT asset. What is new is the scale and relative simplicity of attacks in the Internet of Things (IoT) - the millions and billions of devices that are a potential victim of traditional style cyber-attacks, but on a much larger scale and often with limited or no protection.

The most prevalent devices which are connected to serving IoT applications for infotainment purposes are smart TVs, webcams and printers. A vulnerability analysis has been conducted on these devices using Nessus[1] tool to observe that approximately 13% of the devices out of 156,680 were attributing vulnerabilities which were further classified as critical, high, medium and low. The vulnerabilities that exist in such as MiniUPnP, NAT-PMP detection, unencrypted telnet, Simple Network Management Protocol (SNMP) agents, Secure Shell (SSH) weak algorithms and File Transfer Protocol (FTP) inherited by webcams, smart TVs and printers are further identified based on manufacturer models.

In this section, we present the results of our study on the existing vulnerabilities, exploitable attacks and possible countermeasures in the context of the IoT and the state-of-the-art IoT security. We surveyed a wide range of existing work in the area of IoT security that uses different techniques. We classified the IoT security attacks and the proposed countermeasures based on the current security threats, considering all three layers: Perception, Network and Application. The Figure 1 illustrates the typical architecture of IoT and entities which are considered under each layer. These attacks and their corresponding solutions will be further discussed below.

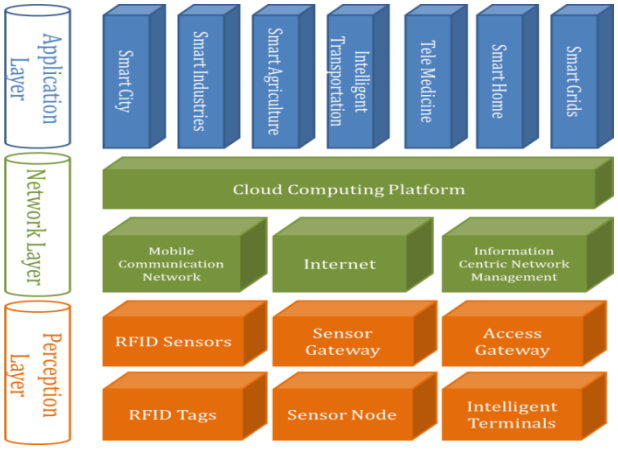

Figure 1 - IoT architecture

Industrial IoT (IIoT)

M2M based automation systems are quite common for industries such as oil and gas manufacturers. These industries are vast and the machinery employed is massive, expensive and poses a significant risk to machine operators. The functions such as oil exploration by drilling, refining and distributing are all conducted using automated machinery controlled through Programmable Logic Controller (PLC) based on SCADA systems. Though, the current M2M infrastructure is ideal for controlling the machinery, remote monitoring and accessibility is limited while a proper data storage and processing mechanism for decision making is unavailable. Thus, the requirement for IoT arises to improve the operational efficiency by optimizing the robot controlling, reducing downtime through predictive and preventive maintenance, increasing productivity and safety through real time remote monitoring of assets. IoT sensor nodes could be deployed at the machinery while monitoring tools could be integrated without affecting the operation of SCADA systems. Hence, SCADA system could be optimized to enhance the productivity.

Smart Buildings, Environments and Cities

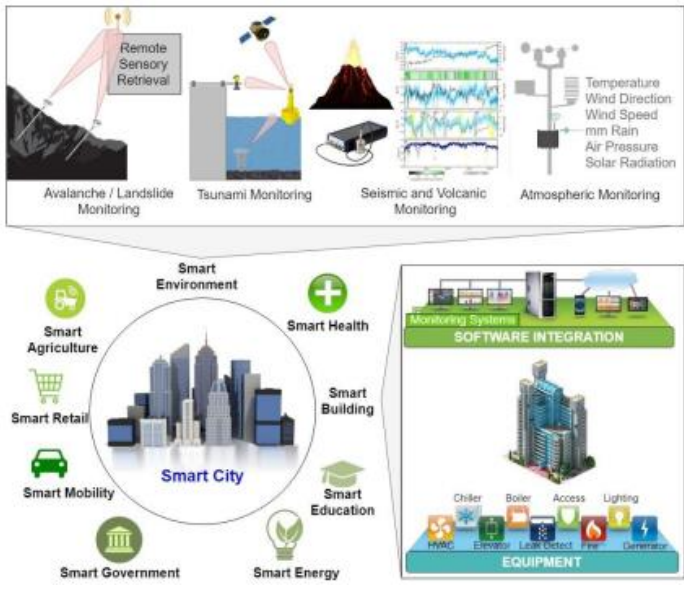

Figure 2 – Smart City Concept

Smart city is a holistically expanded inclusion of smart buildings and smart environments along with other smart automation systems formed for improving the quality of life for residents in a city. This is in fact the most expandable version of any IoT application in terms of cost for infrastructure deployment and geographical extent. In this concept, as shown in Figure 2, sensors are deployed throughout the building, environment or the city for the purpose of extracting data of parameters varied from temperature, humidity, atmospheric pressure, air density / air quality, noise level, seismic detection, flood detection and radiation level. CCTV streams and LPSs would be a valuable input for smart building and smart cities for detecting intrusions, monitoring traffic and emergencies. All other smart systems explained in the previous sections are in fact subsystems of a functional smart city.

Due to various parameters to be gathered from the sensory acquisitions, heterogeneity is immense and the implementation is arduous. At the same time, management of the gathered Big Data content is not scalable. Thus, providing security for all the applications in smart cities would be extremely challenging. Most of the Big Data content extracted from the sensors is forwarded to clouds through M2M authentication. Due to large data transmissions, cryptographic schemes should be lightweight and the authentication mechanism should be dynamic. DoS or DDoS attacks are most probable and could be mitigated with a strong authentication mechanism [1]. Individual sensors could be compromised to initiate fake emergencies and access control methods should be improved to avoid such inconsistencies at sensor level.

IV. AUTHENTICATION AND AUTHORIZATION

Authentication and access control mechanisms hold a great deal of significance in IoT. Without a proper mechanism for access control, entire IoT architecture could be compromised, since IoT devices are highly reliant on the trustfulness of the other components that are connected with. Thus, a proper access control mechanism is paramount to mitigate the flaws in the current IoT infrastructure.

Access control mechanisms are comprised of two stages (Figure 3) : (1) Authentication and (2) Authorization.

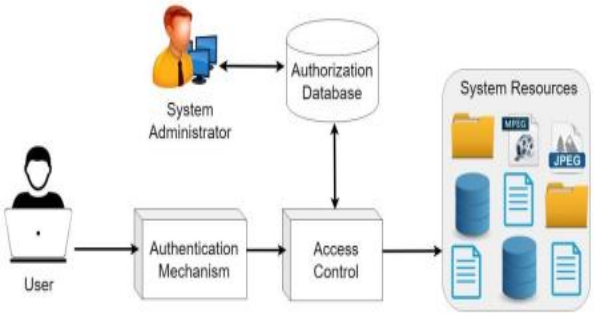

Figure 3 – Typical Access Control System

AUTHENTICATION

Authentication is the process of verifying the identity of an entity [2]. The entity to be verified could either be a human or a machine. Authentication is the first phase of any access control mechanism which can determine the exact identity of the accessing party in order to establish the trust of the system. In most cases, authentication is initiated between a human and a machine in process to log into the internet banking portal entering the credentials. However, in this scenario the access seeking entity does not have a guarantee regarding the identity of the access granting entity. In order to overcome this concern, mutual-authentication should be established between the entities, by verifying the identity of the access granting entity with the involvement of a TTP, such as a Certificate Authority (CA) [2]. CAs are globally recognized institutions which are responsible for issuing and maintaining secure digital certificates of web entities registered under them. These certificates are imperative for the operation of all modern day authentication protocols such as SSL/TLS, IPSec and HTTPS.

The process of authentication is merely facilitating credentials of an entity to the access granting system, which are unique to that entity and could only be possessed by them. This mechanism could be enabled with or without a TTP. The credentials used are often categorized as factors. The authentication schemes accuracy and efficiency depends on the number of factors that are engaged in the mechanism. The types of factors are listed below.

- Knowledge factor – passwords, keys, PINs, patterns
- Possession factor – Random Number Generators (RNG), ATM card, ID card
- Inherence factor – Biometrics such as fingerprint, palm print, iris, etc.

Recent innovations in embedding biometric sensors to smart handheld devices have enabled the possibility of using multi-factor multi-mode (if more than one bio metric is used for verification) Human-to-Machine (H2M) authentication protocols for IoT devices. Though, Machine-to-Machine (M2M) authentication could only be conducted using cryptographic primitives. However, including strong cryptographic primitives (Public Key Infrastructure (PKI), Hashing, Timestamps, etc.) for the authentication protocols involved is crucial in order to ensure data confidentiality, integrity and availability, as the credentials being conveyed are highly sensitive and unique for the authenticating entity.

AUTHORIZATION

Authorization is the process of enforcing limits and granting privileges to the authenticated entities. In simple terms, this is determining the capabilities of an entity in the system. In order for an entity to be authorized for performing any action, the identity of that entity should be verified first through authentication. According to Figure 3, usually an administrator is configuring the authorization database for granting access and rights to system resources. Each resource is assigned with different rights such as read, write and execute. Depending on the level of authorization (clearance) being set by the administrator, each authenticated entity can perform different actions on resources. A typical access control system has a policy for granting rights. These policies could vary from Discretionary Access Control (DAC), Mandatory Access Control (MAC) or a Multi-Level Security (MLS) model such as Role Based Access Control (RBAC). In DAC, the administrator is specifying the rights, while in MAC there are rules set by the system for assigning rights for subjects.

Clearances are granted according to the role of the authenticated entity (Roles: course coordinator, lecturer or student in a university) in RBAC.

V. AUTHENTICATION AT IOT LAYERS

Authentication is the most critical security requirement in IoT for preserving the user identity and mitigating the threats as mentioned in the previous sections. With each IoT application, more hardware devices are introduced to be integrated to the IoT network. The authentication is the mechanism used to ensure the connectivity of those components to the existing ones. Authentication mechanisms involve cryptographic primitives for transmitting credentials securely. The strength of the scheme is entirely dependent on the crypto primitives being used. Though, developing a generic solution would be infeasible, as different layers attribute different requirements in IoT and the resources available for processing, memory and energy are diverse. Therefore, we will discuss the authentication requirements for each layer.

Perception Layer

Perception layer includes all the hardware devices or the Machines to extract data from IoT environments. In most cases the authentication initiates as M2M connections. Thus, in this layer authentication could be conducted either as peer authentication or origin authentication [1]. In peer authentication, validation occurs between IoT routing peers, preliminary to routing information exchanging phase, while validating the route information by the connected peer IoT devices with its source is origin authentication. This method enhances the security in M2M communication. Though as mentioned previously, devices in Perception layer are inheriting inadequate resources for generating strong cryptographic primitives.

Perception Nodes

These nodes are distributed across the IoT environment. Mostly, they are RFID tags and RFID readers / sensors, where few RFID tags are connected to a RFID reader. The connection establishment between RFID tags and the reader does not involve an authentication mechanism and would be vulnerable if the RFID tags can be cloned. Due to resource scarcity, an authentication protocol could be implemented using techniques such as Elliptic Curve Cryptography (ECC) based Diffie-Hellman (DH) key generation mechanism [1]. The generated keys, once they are transmitted to the two ends, could be used as the shared symmetric key for information transferring via the medium securely. However, MiM attacks are still feasible and could be solved employing ephemeral DH method, by changing the ECC DH exponents for each connection establishment as a session key.

Sensor Nodes and Gateways

Sensor nodes face similar security flaws as the perception nodes. Thus, deploying a proper authentication scheme could eliminate the possibility of being exposed to a very low level. However, sensors are much intelligent and resourceful than perception nodes. Hence, M2M authentication could be established as peer authentications and the origin authentication could be established via the sensor gateway. Similarly to the perception nodes, ECC based DH key exchange would be ideal for sensor nodes, where the ephemeral exponents are facilitated by the sensor gateway acting as a TTP. Identity validation of the sensor gateway should be conducted prior to any data transfer. Even though using certificates for identity determination is not practical, a similar parameter such as a serial number could be used when registering the sensor node in the IoT environment and all the identities are stored in the sensor gateway for validation. Sensor gateway should also possess a unique identity for mutual authentication to be established between the sensor node and the gateway. Moreover, countermeasures such as integrity violation detection (using Hashed Message Authentication Code – HMAC or Cipher Block Chaining MAC – CBC-MAC) and timestamps should be employed with the authentication protocols involved.

Network Layer

IoT network layer is integrated on top of the existing TCP/IP internet protocols. In this section we discuss the significance of the authentication for the components of the network layer.

Mobile Communication

Security for mobile communication at network layer was not a critical necessity until the inception of IoT, as most of the mobile applications were relying on the inbuilt security protocols of the corresponding mobile technology (such as Global System for Mobile Communication - GSM, Wireless Code Division Multiple Access - WCDMA, High Speed Packet Access - HSPA or Long Term Evolution - LTE). With IoT, inbuilt authentication schemes are no longer foolproof, considering the potentiality for integrating technologies embedded in addition to the mobile technologies. Current security level and comprised resources (such as processor, memory and operating system) in mobile devices are adequate for designing tamper resistance authentication protocols at the network layer. However, the existing key generation algorithms used in TCP/IP protocols for generating large and costly asymmetric keys (RSA, ElGamal or Paillier), are still not feasible to be used with mobile devices. Thus, generating unbreachable and lightweight keys would be the most challenging task in mobile communication.

Current mobile devices include different biometric sensors for extracting biometrics such as fingerprint, iris, facial and voice imprints. Biometrics can be used as unique keys that could be used for authentication and can be employed with H2M authentication. As majority of the mobile devices at operation in an IoT environment are handled by a human user, the authentication design and the keys generation could be based on biometrics. The security of the biometrics schemes could be enhanced using several biometrics (multi-mode) integrated into multi-factor authentication schemes. These biometrically generated keys could be used as the signatures of each mobile entity for the verification of their identities and for conveying a secure session key among the communicating parties with proper encryption schemes. Additionally, authentication credentials should be checked for probable integrity violations in order to avoid MiM attacks.

Cloud Computing

Clouds are the storage facility of IoT architecture and they are quite resourceful in terms of memory and processing. Thus, authentication should employ strong keys that are generated using public-key algorithms such as RSA or ElGamal, which are inviolable cryptographic primitives if the executing authentication mechanism are computationally feasible with the available resources. A symmetric key (AES, TDES, etc.) to be used in data transferring between the IoT devices and the cloud could be generated and shared among the entities that are engaged in a communication. Existing CAs could be used to validate the identity of the parties involved in communication via mutual authentication schemes for establishing the trust.

The authentication schemes would be more secure in these schemes, as blockchain support pseudonymity (the nodes are identified from hashes or public keys – CA not required and simplify the authentication scheme) and the homomorphism facilitates additional layer of encryption to secure the communication.

VI. CONCLUSION

Authorization techniques in clouds should be also be considered, as accessing the information in the clouds is vital for the IoT design. Existing access control mechanisms such as RBAC and MAC are not scalable and interoperable anymore. Thus, a novel method called Capability-Based Access Control (CapBAC), which uses capability based authority tokens to grant privileges to entities. However, the main concern in cloud computing is the privacy of the user data. A strong authentication scheme does not ensure the misusing of information by the CSP. Thus, approaches such as blockchain and homomorphism should be considered for enhancing the privacy.

VII. REFERENCES

[1]. Qin E, Long Y, Zhang C, Huang L (2013) Cloud computing and the Internet of Things: technology innovation in automobile service. In: International Conference on Human Interface and the Management of Information. Springer, pp 173–180

[2]. Francillon A, Danev B, Capkun S (2011) Relay attacks on Passive Keyless Entry and Start Systems in modern cars. In: Proceedings of the 18th Annual Network and Distributed System Security Symposium. The Internet Society. Citeseer

[3]. Vivek Thoutam, "Unique Security Challenges of IoT Devices and Spectrum of Security Considerations", Journal of Artificial Intelligence, Machine Learning and Neural Network, Vol 01, No. 2, Oct-Nov 2021

[4]. Qiuping W, Shunbing Z, Chunquan D (2011) Study on key technologies of Internet of Things perceiving mine. Procedia Eng 26:2326–2333

[5]. Hernandez G, Arias O, Buentello D, Jin Y (2014) Smart Nest thermostat: a smart spy in your home, Black Hat USA

[6]. Ling Z, Liu K, Xu Y, Jin Y, Fu X An end-to-end view of IoT security and privacy

[7]. Vasundhara D.N, Seetha M, "Rough-set and artificial neural networks-based image classification", 2nd International Conference on Contemporary Computing and Informatics (IC3I) 2016, 35-39.

[8]. D.N. Vasundhara, M. Seetha, "Accuracy assessment of rough set based SVM technique for spatial image classification", International Journal of Knowledge and Learning, Vol. 12, No. 3, 2018, 269-285.

[9]. Dr. R. LAKSHMI TULASI, M.RAVIKANTH, "Intrusion Detection System Based On 802.11 Specific Attacks", International Journal of Computer Science & Communication Networks, Vol 1, Issue 2, Nov 2011

[10]. Peddyreddy. Swathi, "Architecture And Editions of Sql Server", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 4, May-June-2017

[11]. Dr. R. LAKSHMI TULASI, M.RAVIKANTH, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", International Journal of Computer Trends and Technology, July-Aug 2011

Cite this article as :

Bharath Alli, "An Extensive Study on Authentication and Authorization of IOT Devices", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 443-452, November-December 2021.

Journal URL : https://ijsrcseit.com/CSEIT228223