VIVA-Tech International Journal for Research and Innovation
ISSN(Online): 2581-7280

Volume 1, Issue 4 (2021)
Article No. X
PP XX-XX

VIVA Institute of Technology
9th National Conference on Role of Engineers in Nation Building – 2021 (NCRENB-2021)

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

A survey on Internet of Things (IoT) security : Challenges and Current status

Bhavika Thakur[1]
[1]*Computer Engineering Department, VIVA Institute of Technology, India*

Abstract : *When Internet of Things (IoT) applications become a part of people's daily life, security issues in IoT have caught substantial attention in both academia and industry. Compared to traditional computing systems, IoT systems have more inherent vulnerabilities, and in the intervening time, could have higher security requirements. However, the current design of IoT does not successfully address the higher security requirements postured by those vulnerabilities. Many recent attacks on IoT systems have shown that novel security solutions are needed to defend this emerging system. This paper purposes to examine security challenges resulted from the special characteristics of the IoT systems and the new features of the IoT applications. This could help pave the road to better security solution design. Furthermore, three architectural security designs are suggested and analyzed. Examples of how to implement these designs are discussed. Finally, for each layer in IoT architecture, open issues are also identified.*

Keywords - *Architecture IoT, Challenges, Internet of Things, Open issues, Security*

I. INTRODUCTION

Internet of things (IoT) is a group of many interrelated objects, services, humans, and devices that can communicate, share data, and information to achieve a common goal in different regions and applications. IoT has many execution domains like transportation, agriculture, healthcare, energy production and distribution. Devices in IoT keep an eye on an Identity Management approach to be recognized in a collection of similar and heterogeneous devices. Similarly, a region in IoT can be defined by an IP address but within each region each entity has a unique.

The purpose of IoT is to change the way we live today by making smart devices around us carry out daily tasks and responsibilities. Smart homes, smart cities, smart transportation and infrastructure etc. are the terms which are used in application with IoT. There are many application domains of IoT, ranging from personal to enterprise environments [1]. The uses in individual and social domain facilitate the IoT users to interact with their surrounding environment, and human users to maintain and build social relationships. An additional application of IoT is in transportation domain, in which several smart cars, smart roads, and smart traffic signals function the purpose of safe and suitable transportation facilities. The enterprises and industries domain incorporate the applications used in finance, banking, marketing etc. to enable different inter- and intraactivities in organizations. The latter application domain is the service and utility monitoring sector which be made up of agriculture, breeding, energy management, recycling operations, etc.

The IoT applications have seen rapid development in recent years due to the technologies of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN). The RFID permits the tagging or marking of every single device, so as to function as the basic identification mechanism in IoT. Due to WSN, each "thing" i.e. people, devices etc. becomes a wireless recognizable object and can interconnect among the physical, cyber, and digital world [1].

The rest of this paper is structured as follows. In Section II, the security issues corresponding to dissimilar security principles and the nature of IoT devices are presented. The section also contains the security issues that are associated with each layer of IoT. Section III deliberates recent research that attempt to address the security issues in IoT by some countermeasures. Section IV gives the big picture of all the examined work done in IoT. Finally, the paper is concluded in Section V.

II. IOT SECURITY ISSUES

Distinctive security goals of Confidentiality, Integrity and Availability (CIA) also apply to IoT. On the other hand, the IoT has several restrictions and limitations in terms of the components and devices, computational and power resources, and even the heterogonous and ubiquitous nature of IoT that introduce additional concerns. This section contains of two parts: the common security features that the IoT must have, and the security issues explicit to each layer of the IoT.

A. The Security Features of IoT

The security challenges of IoT can be generally divided into two classes; Technological challenges and Security challenges [5]. The technological challenges rise due to the heterogeneous and pervasive nature of IoT devices, while the security challenges are related to the principles and functionalities that should be applied to achieve a secure network. Technological challenges are typically related to wireless technologies, scalability, energy, and distributed nature, while security challenges require the ability to ensure security by authentication, confidentiality, end-to-end security, integrity etc. Security should be enforced in IoT during the course of the development and operational life span of all IoT devices and hubs [4]. To ensure security there are different mechanisms as follows:

- When an IoT device is turned on, it should primary authenticate itself into the network before collecting or sending data.
- The software running on all IoT devices should be authorized.
- Since the IoT devices have limited computation and memory capabilities, firewalling is necessary in IoT network to filter packets directed to the devices.
- The updates and patches on the device should be installed in a way that additional bandwidth is not consumed.

Given below are the security principles that should be enforced to achieve a secure communication framework for the people, software, processes, and things.

1) Confidentiality:

It is very significant to make assured that the data is secure and only accessible to authorized users. In IoT a user can be human, machines and services, and internal objects and external objects (devices that are not part of the network). For example, it is crucial to make sure that sensors don't expose the collected data to neighboring nodes [6]. One more confidentiality issue that must be addressed is how the data will be managed. It is important for the users of IoT to be aware of the data management mechanisms that will be applied, the process or person responsible for the management, and to make sure that the data is protected throughout the process [7].

2) Integrity

The IoT is based on changing data between many different devices, which is why it is very important to ensure the accuracy of the data; that it is coming from the right sender as well as to ensure that the data is not tampered during the development of transmission due to intended or unintended interloping. The integrity feature can be imposed by maintaining end-to-end security in IoT communication. The data traffic is managed by the use of firewalls and protocols, but it does not guarantee the security at endpoints because of the characteristic nature of low computational power at IoT nodes.

3) Availability

The vision of IoT is to link as many smart devices as possible. The users of the IoT should have all the data available whenever they need it. However data is not the only component that is used in the IoT; devices and services must also be reachable and available when needed in a timely manner in order to achieve the expectations of IoT.

4) Authentication

For each object in the IoT must be able to clearly identify and authenticate other objects. However, this process can be very challenging because of the nature of the IoT; many entities are involved (devices, people, services, service providers and processing units) and one other thing is that sometimes objects may need to interact with others for the first time (objects they do not know) [8]. Because of all this, a mechanism to mutually authenticate entities in every interaction in the IoT is needed.

5) Lightweight Solutions

Lightweight solutions are a unique security feature that is bring together because of the restrictions in the computational and power capabilities of the devices involved in the IoT. It is not a goal in itself rather a restriction that must be considered while designing and implementing protocols either in encryption or authentication of data and devices in IoT. Since these algorithms are meant to be run on IoT devices with limited capabilities, so they ought to be compatible with the device capabilities.

6) Heterogeneity

The IoT connects different entities with different capabilities, complexity, and different vendors. The devices even have different dates and release versions, use different technical interfaces and bitrates, and are designed for an altogether different functions, therefore protocols must be designed to work in all different devices as well as in different situations [2, 4, 8]. The IoT aims at connecting device to device, human to device, and human to human, thus it provides connection between heterogeneous things and networks [5]. One more challenge that must be considered in IoT is that the environment is always changing (dynamics), at one time a device might be connected to a completely different set of devices than in another time. And to ensure security optimal cryptography system is needed with an adequate key management and security protocols.

7) Policies

There must be rules and principles to ensure that data will be managed, protected, and transmitted in an efficient way, but more importantly a mechanism to enforce such polices is needed to ensure that every entity is applying the standards. Service Level Agreements (SLAs) must be clearly identified in every service involved. Current policies that are used in computer and networks security may not be applicable for IoT, due to its heterogeneous and dynamic nature. The enforcement of such rules will introduce trust by human users in the IoT paradigm which will eventually result in its growth and scalability.

8) Key Management Systems

In IoT, the devices and IoT sensors need to exchange some encryption materials to ensure confidentiality of the data. For this purpose, there needs to be a lightweight key management system for all frameworks that can enable trust between different things, and can distribute keys by consuming devices' minimum capabilities.

B. Security Challenges in Each Layer of IoT

Each IoT layer is susceptible to security threats and attacks. These can be active, or passive, and can originate from external sources or internal network owing to an attack by the Insider [1]. An active attack directly stops the service while the passive kind monitors IoT network information without hindering its service. At each layer, IoT devices and services are susceptible to Denial of Service attacks (DoS), which make the device, resource or network unavailable to authorized users.

III. IOT SECURITY COUNTERMEASURES

IoT needs security measures at all three layers; at physical layer for data gathering, at network layer for routing and transmission, and at application layer to maintain confidentiality, authentication, and integrity [4]. In this section the state-of-art security measures that address the specific features and security goals of IoT are discussed.

A. Authentication Measures

In 2011, Zhao et al. in [10] presented a mutual authentication scheme for IoT between platforms and terminal nodes. The structure is based on hashing and feature extraction. The feature extraction was combined with the hash function to avoid any collision attacks. This scheme actually provides a good solution for authentication in IoT. The feature extraction process has the properties of irreversibility which is needed to ensure security and it is light weight which is desirable in IoT. The scheme focuses on authentication process when the platform is trying to send data to terminal nodes and not the opposite. Although the scheme will improve the security while keeping the amount of information sent reduced, it works only on theory and there is no practical proof to support it.

Alternative method for ID authentication at sensor nodes of IoT is presented by Wen et al. in [9]. It is a one-time one cipher method based on request-reply mechanism. This dynamic variable cipher is executed by using a pre-shared matrix between the communicating parties. The parties can generate a random coordinate which will serve as the key coordinate. Key coordinate is the thing which actually gets transmitted between two parties, not the key itself. The key, i.e. password, is then created from this coordinate. All the messages are sent by encrypting them with the key, along with key coordinate, device ID, and time stamp. The two devices communicate by validating timestamps, and thus they can cancel the session based on it. This cipher can be used where securing IoT is not very sensitive and crucial because key can be repeated for different coordinates. If key coordinate is changed regularly, security can be optimized for that particular IoT framework. The installation of pre-shared matrix needs to be secure for this work to be implemented for a large number of IoT devices.

Constructing correct access controls is as important as authentication for security, and these two functionalities go hand in hand in securing IoT. To address these functionalities, Mahalle et al. [5] presented an Identity Authentication and Capability based Access Control (IACAC) for the IoT. This research attempts to fill the gap for an integrated protocol with both authentication and access control capabilities to achieve mutual identity establishment in IoT. The proposed model uses a public key approach and is compatible with the lightweight, mobile, distributed, and computationally limited nature of IoT devices and over existing access technologies like Bluetooth, 4G, WiMax, and Wi-Fi. It prevents man-in-the-middle attacks by using a timestamp

in the authentication message between the devices, which serves as the Message Authentication Code (MAC). The structure works in three stages; first a secret key is produced based on Elliptical Curve Cryptography-Diffie Hellman algorithm (ECCDH) [11], then identity establishment is made by one-way and mutual authentication protocols, and lastly access control is implemented. The shared secret key is formed by the combination of public key and a private parameter, and has small size and low computational overhead due to the use of Elliptic Curve Cryptography (ECC). The access is granted by storing a capability with access rights, device identifier, and a random number in each IoT device. This random number is the result of hashing device ID with access rights. The IACAC model does not completely prevent DoS attacks. However, it minimizes it since access of resource is granted to only one ID at a time.

Most of the devices involved in the perception layer of the IoT are RFID and sensors. Such devices have extremely limited computational capability, which makes it tough to apply any cryptography algorithms to ensure the security of the network. However, researchers in [12] introduced a light weight authentication protocol to secure RFID tags. In unsecured RFID the attacker can gain access to the network by sniffing the Electronic Product Key (EPC) of the victim tag and program it to another tag. By applying the authentication protocol such attacks can be prevented. The protocol ensures mutual authentication between RFID readers and tagged items without introducing large overhead on these devices.

B. Trust Establishment

Since, devices in IoT can physically move from one owner to another, trust should be established between both owners to enable a smooth transition of the IoT device with respect to access control and permissions. The work in [13] presents the concept of mutual trust for inter-system security in IoT by creating an item-level access-control framework. It establishes trust from the creation to operation and transmission phase of IoT. This trust is established by two mechanisms; the creation key and the token. Any new device which is created is given a creation key by an entitlement system. This key is to be applied for by the manufacturer of the device. The token are created by the manufacturer, or current owner, and this token is combined with the RFID identification of the device. This mechanism ensures the change of permissions by the device itself if it is assigned a new owner, or it is going to be operated in a different department of the same company, thus reducing the overhead of the new owner. These tokens can be changed by the owners, provided that old token is provided, so as to supersede the permissions and access control of the previous one. This mechanism is similar to changing the old key when a new home is bought.

C. Federated Architecture

Not having universal policies and standards to control the design and the implementation of algorithms in IoT makes it tough to control the security. It is important for IoT architecture to have a federated architecture that has an internal autonomy or centralized unit to overcome the heterogeneity of various devices, softwares and protocols. The work presented in [14] suggested a definition for federated IoT, and based on that definition an access control delegation model is presented. The existing model takes into consideration the flexibility and scalability that are key features in IoT systems. Another such attempt was prepared in [15] to propose a framework called Secure Mediation GateWay (SMGW) for critical infrastructures. This approach is an abstraction of IoT as it is relevant for any kind of distributed infrastructures that are completely different in their nature and operation. SMGW can discover all the relevant distributed information from different nodes, and can overcome the heterogeneity of heterogeneous nodes whether it is a telecommunication, electrical, water distribution node, and can exchange all the messages and information over the untrusted network of Internet. This work enabled the follow-up of another federated approach, presented in [4] to provide the framework of Smart Home based on the SMGW.

It is not enough to have rules and standards to ensure security, mechanisms to enforce such policies are also needed. The research by Neisse et al. in [16] addresses this issue by integrating a security toolkit named SecKit with the MQ Telemetry Transport protocol. The current policies may not be efficient in IoT because of its dynamic nature. The proposed policy mechanism can have good impact in ensuring the security of the IoT, however it introduced additional delay in the process.

D. Security Awareness

Another important security measure for the success and growth of IoT framework is the awareness among human users which are a part of the IoT network. In [17] the authors illuminated the consequences of not securing the IoT using actual numbers. They get into IoT devices (SCADA devices, traffic control devices, web cameras, and printers) that were openly available using either no-password or the default password. The recorded results were very interesting and showed that many of these devices were actually accessible. If people continued with the same unawareness towards security, and used the minimum amount of security like default password that comes with the product, this would make the IoT to cause more harm than good. Hackers can conduct attacks against the whole network if one of its devices is not secured.

IV. CURRENT STATUS OF RESEARCH

IoT security is determined by the various factors and security principles discussed previously, and the challenges that are faced by IoT security has been the focus of many researchers. In this section, an analysis of some related work is presented and the contribution of this paper is given.

In the survey paper presented by Roman et al. in [7], a complete introduction about the IoT and security issues along with the need to have IoT standards are included. Though, no countermeasures are provided for the given security challenges. This work was followed by the survey analysis in [8] in which countermeasures are provided for all security challenges. However, global policies for securing IoT and computational resources of security solutions w.r.t. devices are not provided. The work in [2] attempts to describe the security issues at each layer with certain security measures. But no solution is given except for encryption in the perception layer. The analysis in [1] addresses the security threats, challenges, and requirements in detail, but presents state-of-art countermeasures for only one security feature of access control. In [6], IoT security in terms of the main ethics of security like confidentiality, integrity, and availability are addressed only. The authors recommended two-step authorization using biometrics which is not applicable in case of machine-tomachine communication. The suggested measures are not detailed and do not address the specific nature of IoT with low power heterogeneous devices and huge network traffic. A marvelous survey for IoT, Web of Things (WoT), Social Web of Things (SWoT) is presented in [18], in which security issues, measures and potential research information is given. In this survey paper, the security challenges, requirements, and stateof-art measures and research are presented with emphasis on using the latest network protocols like IPv6 and 5G to further secure the IoT paradigm.

The survey of state of art technologies to secure IoT shows that while many provide countermeasures to cope up with different security challenges, most of them are limited to authentication, identity establishment, and access control functionalities.

Wireless Internet Service Provider (WISPr) roaming and RADIUS are existing solutions to provide authentication and authorization in IoT by means of Wi-Fi over the Internet. Nowadays, many smart devices support IPv6 communications, but the existing deployments in IoT might not support it , and thus necessitates ad hoc gateways and middlewares [19]. The survey shows that open research challenges are present to achieve centralized autonomy in IoT devices by having a Management Hub which manages the identification management issues in IoT.

V. CONCLUSION

The IoT framework is susceptible to attacks at each layer; hence there are many security challenges and requirements that must be addressed. Present state of study in IoT is mainly concentrated on authentication and access control protocols, but with the rapid advancement of technology it is important to incorporate new networking protocols like IPv6 and 5G to achieve the dynamic mashup of IoT topology.

The major developments witnessed in IoT are mainly on small scale i.e. within companies, some industries etc. To scale the IoT framework from one company to a group of different companies and systems, various security concerns need to be overcome. The IoT has countless potential to transform the way we live today. But, the foremost concern in realization of completely smart frameworks is security. If security concerns like privacy, authentication, confidentiality, access control, end-to-end security, trust management, global policies and standards are addressed completely, we can witness the transformation of everything by IoT in the near future. There is need for new identification, wireless, software, and hardware technologies to resolve the currently open research challenges in IoT like the standards for heterogeneous devices, implementation of key management and identity establishment systems, and trust management hubs.

REFERENCES

[1] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.
[2] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.
[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.
[4] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.
[5] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.
[6] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.
[7] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.
[9] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.
[10] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference on Modelling, Identification and Control (ICMIC), 563-566, 2011.
[11] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.
[12] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.
[13] Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.
[14] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capabilitybased access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608, 2012.
[15] M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5, 86-97, 2012.
[16] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.
[17] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," in Joint Intelligence and Security Informatics Conference (JISIC), 232-235, 2014.
[18] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for Interaction with Things on Internet and Underlying Issues," Ad Hoc Networks, 2015.
[19] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, 146-164, 2015.
[20] W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," Wireless Communications, vol. 21, 106-112, 2014.
[21] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," Communications Magazine, vol. 53, 28-35, 2015.