A Comprehensive Review for Security Analysis of IoT Platforms

Chandrashekhar Uppin *cvuppin@gmail.com*
HOD, Department of Computer Science,
Faculty of Computing and Applied Sciences,
Baze University, Jabi Abuja, Nigeria

Sudhir Anakal *sudhir.anakal@gmail.com*
Department of Studies in Computer Applications,
Visvesvaraya Technological University,
Postgraduate Centre, Kalaburagi, India

Abstract

Due to the rapid growth in the field of science and technology, IoT (Internet of Things) has become emerging technique for connecting heterogeneous technologies related to our daily needs that can affect our lives tremendously. It allows the devices to be connected to each other and controlled or monitored through handheld devices. The IoT network is a heterogeneous network that links several small hardware restriction devices, and where conventional security architectures and techniques cannot be used. So, providing protection to the IoT network involves a diverse range of specialized techniques and architectures. This paper focuses on the requirements of defense, current state of the art and future directions in the field of IoT.

Keywords: Internet of Things, Security Requirements, IoT Platforms, Information Security, IoT Security.

1. INTRODUCTION

Ultimately, in today's world where technology is progressing at a far higher pace, cyber-attacks have now become a fact of life, with high-profile company data breaches and organizations making headlines almost daily news.

The idea of IoT came about in the 1970s but as a result of the Internet of Things (IoT) business development[1] attracted the attention of researchers and data scientists. The era of the IoT (Internet of Things) that can be incorporated into the smart vehicle, smart house, smart building and smart city is coming because of the exponential growth of network infrastructure and sensor. IoT is a very beneficial environment that offers a range of resources (e.g., amazon echo), but at the same time risk can be enormous too. Gartner, Cisco, and IDC (International Data Corporation) identify IoT as a promising future technology, and most of the company also agree that IoT will become a gateway to their next-generation growth potential. The size of the IoT market is expected to rise from $655.8 billion in 2014 to $1.7 trillion in 2020 with an annual compound growth rate of 16.9 per cent[2], according to IDC. The growing complexity of IoT networks also magnifies the security problems faced by these networks. Attacks in IoT are possible because the devices in the IoT network are an simple intrusion target [3].

When IoT networks are increasingly critical to their mission, issues such as durability, safety, safety, complex structure, and semi-or even full-automated system recombination and/or reconfiguration are important. Not only will responsiveness accelerate the creation of new architectures on the IoT platform, it will also generate fresh and unimagined opportunities and requirements.

IoT platform provides a new category of cyber security risk for society that is already facing a Iot

of hacks and breaches of data. The key safety features of any IoT system are-

1) IoT system should be able to recognise when linked to a network by its unique address. Manipulating a single node in interconnected environments can create security issues about data integrity.
2) IoT system will only allow approved users to access configuration rights or firmware updates.
3) IoT system should be able to secure the data it stores or transmits over the networks using advanced encryption techniques.
4) Software or firmware for IoT devices should be modified using secure mechanism.
5) IoT system should be able to create an event log for investigation, if necessary.

2. RELATED WORK

Due to the different characteristic of the devices connected with it as well as the distributed aspect of the communication medium, IoT networks are more vulnerable to the security threat. It also has an inherent drawback, as nodes are often placed in an open environment [3,4]. Consequently, the popularity of IoT services is certainly increasing [5], fostering as well intensive research on this new field. Nonetheless, developing applications in the IoT context may represent a cumbersome task, mainly due to the following challenges:

- Lack of detailed documentation of current frames
- Several programming languages for managing the machines
- Software the systems are heterogeneous
- Resource limitations inherent in the IoT Nodes
- The systems use various communication protocols.

The IoT technologies are in continuous expansion as described earlier. Consequently, many research papers have been published recently aimed at surveying the IoT domain from various perspectives. In this context, a survey is provided in [6] on enabling technologies, protocols, and application problems. The main objective of this work is to provide an overview of the above-mentioned challenges to endow researchers and developers with a simple overview of how to combine the different protocols to deliver IoT solutions without going deep into the specifics of the protocols. Similarly, after surveying the enabling technologies, the authors in [7] suggested key IoT applications that could support industries such as healthcare, the food supply chain and many others.

Authors in [8] studied many market-level IoT approaches to argue about future applications and technologies used. In particular, they defined developments in IoT solutions based on the market, classifying them into five separate categories, namely: smart wearable, smart home, smart city, smart environment and smart business. In addition, Ganguly[9] compared IoT solutions in the cloud based on four factors: technology offerings, strategy, market presence and compliance. That factor contains sub-factors, so the author may conclude on the benefits of following a particular framework with generic statements. Two security features are evaluated during the analysis as a sub-factor of technical offerings, namely security of message level and data encryption. The author obviously believed the protection of the transportation layer is already present.

The new security and privacy evaluations of IoT networks can be found at [10]. e Authors based on privacy in home automation networks allegedly applied to IoT applications. It is shown that both simple cryptographic techniques and data manipulation are used to save a user within the IoT network against a competitor or adversary who has compromised remote servers.

A detailed survey of IoT problems relating to privacy and trust can be found in[11]. Traditional protection countermeasures are very specific and cannot be applied to IoT technologies instantly because of the heterogeneous requirements and communication stacks involved.

In addition, IoT problems are also addressed in[12] where authors introduced industrial IoT and addressed related security and privacy issues, as well as offering viable solutions leading to a comprehensive framework for protection.

Choi et al. [13] introduced device authentication based on the device signature. The device signature used as an input, and then it is divided into equal size fragments and distributed among the network if any device wants authentication verification, a hash verification process done.

Lee et al. [14] introduced a smart and secure home network by focusing on user privacy. This scheme uses all the data security features, which are essentials for data communication in a personal network — this scheme based on the encryption, access control, and digital signature, authentication and logging.

Tomanek et al. [15] introduced a scheme based on the “Alljoyn” Framework. Here in this scheme, all the devices need to authenticate against the given policy before communicating with other devices. Here each device maintains an access control list (ACL) which has all the details of the communicating nodes. Here session management plays an essential role in device communication. No device is allowed to communicate after expiration of the session.

Abdallah et al. [16] planned the light-weight lattice-based homomorphic privacy-preserving aggregation theme that accustomed cipher the message between the devices. This scheme splits the network into separate lattice, and those lattices connected with individual AP's. These AP's then communicate with others, ensuring privacy preservation during message transmission and provides robust encryption also.

Mantoro et al. [17] proposed an algorithm for monitoring smartphones communication using hash chain-based scheme. The algorithmic rule uses AES256, Diffie-Hellman key exchange, and RC4-based hash algorithm. This algorithm follows the Ring Topological structure, here in this all messages are transmitted through the central Hub, and easy monitoring is possible.

Won Min Kang [18] uses the auto-signing and access management technique for removal of safety attacks like information modification, outflow and code fabrication. During this paper, any new module added to the smart home network can perform linguistic communication validation from the authentication module, and once the whole authentication materialized, it will generate a certificate solely then it is allowed for taking part within the communication method.

Hua Mao [19] uses the concept lattice technique for attribute reduction by using matroidal theory. In this paper only selected attributes of a lattice that are enough to represent information. The concept of the lattice is breakdown into different subsets, and each subset is mapped with another subset element so that attributes gets minimized.

Hua Mao [20] discusses the concept of lattice-based on a set-theoretical model for concept and conceptual hierarchies. In this paper, a universal set classified into three regions known as “trisection”. It uses attribute reduction concepts and generates a concept lattice.

Yi Yu Yao [21] discusses the concepts of three-way decision; this approach signifies that each problem decision classified into three regions positive, negative and non-commitment. The three-way decision theory helps in determining whether this problem belongs to the specified category and determine the solution of the concerned problem. This approach is beneficial when there is an ambiguity in decision-making for a specific problem.

Xiaonan Li [22] introduced generalized mataroids based three-way decision models. It first introduced the three-way decision model based on subset evaluation and proposed a rough set theory that enables the attribute reduction approach on a lattice that helps represent information in a minimum possible attribute.

3. SECURITY REQUIREMENTS OF IOT PLATFORMS

3.1. Confidentiality: The confidentiality clause states that the information must be kept confidential. Since the IoT network has built-in wireless functionality, it may be possible that the information must be leaked over the wireless network, so a firm encryption policy is required to protect data.

3.2. Privacy: Privacy clause states that personal information must not be made publicly available. Since devices interconnected to each other, there exist a privacy issue.

3.3. Integrity: Data must not be changed until the change is needed or required for the purpose. Since IoT network relies on the wireless medium, it may be possible that an intruder can inject malicious code into the network and compromised it, so a token mechanism required for data communication [10-12].

3.4. Availability: Availability clause states that the information must be available when there is a need for the information. If a network compromised by an attacker, it may be possible that it can modify the data that modified data can cause damage to the network. So, a strong access control policy needed for data communication [13,14,15,10].

3.5. Non- Repudiation: Non-repudiation clause states that the sender cannot deny sending the information and the receiver cannot deny when it is received.

3.6. Authentication: There should be proper authentication of the sender as well as the receiver. For maintaining the proper authentication between sender and receiver, a token must implement so that it can authenticate the legitimate sender or receiver.

4. ANALYSIS OF CHARACTERISTIC OF IOT PLATFORMS

This section analyzes security specifications based on three standard IoT features that have been studied in other studies. In IoT protection these safety criteria are generally applied. For design protection mechanisms in the IoT setting it is therefore important to understand and take advantage of it.

- **Integration and interoperability:** Since the devices in a smart home network are heterogeneous in nature because there are different mechanisms and prerequisites for each and every system belonging to the same group, there is a problem of how such devices can be related and how they can be controlled.
- **Privacy and Secrecy**: As smart home is connected to the internet and there are several attacks present to the network because smart home network is no different from any other wireless network ,So there is always a risk associated with the wireless network.
- **System Complexity**: Various types of networks exist within a smart home network. For example, wireless sensor network and body area network(BAN), it is very difficult to create contact between these heterogeneous networks due to the presence of these types of networks and that is why the system is more complicated.
- **Bandwidth management**: In the future, traffic volume on the Internet will increase significantly due to smart home applications, because no such successful strategy has existed in such a complex network for bandwidth management. Therefore bandwidth control in a smart home network is also an significant issue.
- **Protocol issues**: Since smart home network consists of heterogeneous components, new communication protocol is required to share information with heterogeneous network types.
- **Cost effectiveness**: Deploying and protecting smart home networks is very costly because this large amount of energy is required, so making it cost-effective and safe in the best possible way is a challenge for smart home networks.
- **Social Impact**: Smart home may have an influence on society, some people may be disconnected from society for example. As a smart house, all the work can be performed automatically without any human involvement. communication between a human and the society where he lives.

5. IOT PLATFORMS OVERVIEW

According to industry research by the Boston Consulting Group, the Internet of Things industry expects to hit $267B spent on IoT technology, goods, and services by 2020[24]. Furthermore, by 2025 the number of smart things will rise to 75.4 billion connected devices: (i) impacting the automation by connecting machines, sensors and actuators to automate industrial processes; (ii) integrating the data from a machine or sensor with the organizational databases and other data sources such as open government databases, social media feeds, etc.; and (iii) moving to a service-oriented business model through the above-mentioned automation and integration processes.

There are many IoT platforms available in the market, thus each and every platform provides smart features but there also exist certain security issues. The Table 1 indicates IoT platforms along with security concerns.

Platform	Security Concern
Samsung Artik	1. Token Based Communication 2. Token can be eailty trapped 3. Poor Authentication
Amazon IoT	1. Cloud based authentication 2. Highly Secured
IBM Watson IoT	1. Cloud based authentication 2. API Based Calling
Oracle IoT	1. Cloud based authentication 2. Certificate Based authentication
Evrythng	PKI Based Authentication
Node-Red	Credentials based authentication
The Thing System	Credentials based authentication,OTP features
Nimbits	Data at rest: cyphering mySQL database
Sitewhere	Devices IoT to cloud: hardware ID and tokens.

TABLE 1 : Parameters Extracted from Network Table.

6. EVALUATION

Together with our work we review work on IoT protection requirements. As seen in Table 1, most work concerns only security standards about privacy, access control (i.e., authentication and authorisation), and security threats. That is, the current work does not cover overall IoT system protection requirements. We first evaluated the basic safety criteria based on the three characteristics in this paper (i.e., heterogeneity, resource constraint, complex environment). Second, on the basis of six elements (i.e. IoT network, cloud, user, intruder, device, platform) in the IoT context, safety, multicasting and bootstrapping in the IoT network, availability, data security, etc. were analysed.

Proposed Framework	Working	Issue Considered	Proposed By
Firmware Validation and Update Scheme	Device Signature-based authentication scheme.	Integrity- 1 Availability- x Authentication-o	Choi(2016)
Defence against Personal information hijacking and burst attacks	Encryption, access control, digital signature, authentication, logging	Integrity- 1 Availability- x Authentication-o	Lee(2016)

All-Joyn Framework	Data is transmitted after authentication between devices. Authenticated devices transmit messages encrypted with a given policy	Integrity- 1 Availability- x Authentication-o	Tomanek(2016)
Lattice-based homomorphic privacy-preserving aggregation scheme	Uses lattice-based homomorphic cryptosystem to encrypt the message	Integrity- 1 Availability- 1 Authentication-x	Abdallah(2014)
Uses encryption Algorithm and Hash-Based function	AES 256+Deffie Hillman key exchange algorithm+RCH Hashed Based Function	Integrity-o Availability-x Authentication-0	Manestoro(2014)
Uses Self Signing along with Authentication Control	Device Self-signed themselves to the authentication Module and then get the Access	Integrity-o Availability- 1 Authentication-0	Won Min Kang (2017)
Attribute reduction using Mataroid theory	In this paper only selected attributes of a lattice that are enough to represent information are considered	Integrity-o Availability- 1 Authentication-0	Hua Mao (2014)
Attribute reduction using concept lattice using graph	Discusses the concept of lattice-based on a set-theoretical model for concept and conceptual hierarchies	Integrity-o Availability- 1 Authentication-0	Hua Mao (2016)
Theory of three-way decisions	Discusses the concepts of three-way decision; this approach signifies that each problem decision can be classified into three regions positive, negative and non-commitment.	Integrity-o Availability- 1 Authentication-0	Yiyu Yao (2012)
Mataroids based on a three-way decision model	. It first introduces a three-way decision model based on subset evaluation and proposed rough set theory that enable attribute reduction approach on a lattice that helps represent information in a minimum possible attribute	Integrity-o Availability- 1 Authentication-0	Xianon Li (2017)
Proposed Framework	Device authentication through Squid Authentication hosted on Cloud through a random token generated token which will expire after a particular timestamp	Integrity-o Availablity-0 Authentication-0	

TABLE 2: Comparison of Existing Framework with Proposed Framework
0-Strong 1 -Medium, x-Weak.

7. CONCLUSION AND FUTURE WORK

We evaluated three main IoT characteristics in this paper, such as heterogeneity, resource constraint, and dynamic setting, in order to find out basic IoT protection requirements. We also evaluated overall IoT security criteria (e.g., privacy, trust, system security control), based on security issues of six core elements in the IoT context and assessment of protection requirements is carried out with many researches. We hope that this paper will be a reference for safely developing the IoT framework and enhancing general understanding of IoT security issues and needs. We need to examine international IoT security standards for interoperability in the future among a lot of diverse security platforms, tools, policies, etc.

8. REFERENCES

[1] H. Kopetz," Internet of things," in Real-Time Systems, ed: Springer,2011,pp.307-323.

[2] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor network deployed for IoT Applications", IEEE Access, vol. 3, pp. 1503-1511, August 2015

[3] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017

[4] N. Aleisa and K. Renaud, "Privacy of the internet of things: a systematic literature review," in Proceedings of 50th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 2017

[5] J. Veijalainen, D. Kozlov, and Y. Ali, "Security and privacy threats in IoT architectures," in Proceedings of 7th International Conference on Body Area Networks, Oslo, Norway, September 2012.

[6] International Data Corporation (IDC), Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC, 02 June 2015, [Online]. Available: http://www.idc.com/getdoc. jsp?containerId=prUS25658015. [Accessed 22 August 2016].

[7] S.-R. Oh, Y.-G. Kim, "Security analysis of MQTT and CoAP protocols in the IoT environment", Korea Information Processing Society (KIPS) South Korea, pp. 297-299, April 2016.

[8] Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376. [CrossRef]

[9] Xu, L.D.; He, W.; Li, S. Internet of Things in Industries: A Survey. IEEE Trans. Ind. Inform. 2014, 10, 2233–2243.

[10] Ganguly, P. Selecting the right IoT cloud platform. In Proceedings of the 2016 International Conference on Internet of Things and Applications (IOTA), Pune, India, 22–24 January 2016; pp. 316–320.

[11] Guth, J.; Breitenbücher, U.; Falkenthal, M.; Leymann, F.; Reinfurt, L. Comparison of IoT platform architectures: A field study based on a reference architecture. In Proceedings of the 2016 Cloudification of the Internet of Things (CIoT), Paris, France, 23–25 November 2016; pp. 1–6.

[12] Derhamy, H.; Eliasson, J.; Delsing, J.; Priller, P. A survey of commercial frameworks for the Internet of Things. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–8.

[13] Choi BC, Lee SH, Na JC, Lee JH (2016) Secure firmware validation and update for consumer devices in home networking. IEEE Trans Consum Electron 62(1):39–44

[14] Lee S, Kim J, Shon T (2016) User privacy-enhanced security architecture for home area network of smartgrid. Multimed Tools Appl 75(2016):12749–12764

[15] Tomanek O, Kencl L (2016) Security and privacy of using AllJoyn IoT framework at home and beyond. 2016 2nd international conference on intelligent green building and smart grid (IGBSG), pp 1–6

[16] Abdallah AR, Shen XS (2014) Lightweight lattice-based homomorphic privacy-preserving aggregation scheme for home area networks. 2014 sixth international conference on wireless communications and signal processing (WCSP), pp 1–6

[17] Mantoro T, Ayu MA, binti Mahmod SM (2014) Securing the authentication and message integrity for smart home using smart phone. 2014 international conference on multimedia computing and systems (ICMCS), pp 1–5.

[18] Lee C, Zappaterra L, Choi K, Choi HA (2014) Securing smart home: technologies, security challenges, and security requirements. Workshop on security and privacy in machine-to-machine communications (M2MSec'14), pp 67–72

[19] Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutor 16(4):1933–1954

[20] Schiefer M (2015) Smart home definition and security threats. 2015 ninth international conference on IT security incident management & IT forensics, pp 114–118.

[21] Jacobsson A, Boldt M, Carlsson B (2016) A risk analysis of a smart home automation system. Future Gener Comput Syst 56(2016):719–733

[22] Jose AC, Malekian R (2015) Smart home automation security: a literature review. Smart Comput Rev 5(4):269–285.

[23] U. Saxena, J. S. Sodhi and Y. Singh, "Analysis of security attacks in a smart home networks," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, pp. 431- 436, 2017.

[24] Hunke, N.; Rüßmann, M.; Schmieg, F.; Bhatia, A.; Kalra, N. Winning in IoT: It's All about the Business Processes. Available online:https://www.bcg.com/en-co/publications/2017/hardware-software-energyenvironment-winning-in-iot-all-about-winning-processes.aspx (accessed on 25 October 2018).