A Comparative Study on Models and Techniques for Securing IoT Applications

Abdullah Mohammed Alsaedi
Faculty of Computer Science and Engineering
Taibah University

ABSTRACT
With digitization continuing to enter all aspects of daily life, a growing number of devices and appliances are becoming 'smart' and digitally connected. As a result, a large range of IoT applications have been developed and released utilizing a variety of IoT frameworks. All frameworks of IoT environments are composed of a set of procedurals, rules and standards that allow easy implementation and deployment of the various IoT applications. Deploying and implementing these applications necessitates a range of mechanisms and procedurals of security and privacy to ensure proper working and avoid any threats that may occur. This paper introduces a survey of how to secure IoT frameworks through applying a comparative study on a set of basic security mechanisms applied by providing background about security mechanisms, in addition to advantages and disadvantages of each security technique in IoT applications domain.

Keywords
Internet of Things, Security mechanism, Security architecture

1. INTRODUCTION
"The Internet of Things (IoT)" is strongly enrolled in many various applications, different frameworks and domains in our daily lives from small device applications to large industrial systems. IoT represents a critical part and role in many different daily life applications such as industry environments, healthcare and communications. Nowadays, IoT is enrolled in most of our daily activities and how people interact with the surrounding environment. For this reason, the importance and need to achieve secure IoT applications can be considered essential and is required to ensure privacy and security for users. As a result of the importance and need of such applications in our life, we move towards a deeper understanding of the IoT environment and its challenges to be able to propose such applications that are easy to use and free of any threats and mistakes. IoT applications face many challenges and difficulties, such as that it is written by many programming languages and uses different protocols, so it is applicable to good treatment with such issues and introduce such security mechanism that prevent any threats or attacks that may occur.

The rest of the paper is organized as follows: Section 2 introduces a brief description of IoT architecture and basic characteristics of IoT applications. Section 3 gives the main challenges of IoT application security. Section 4 surveys current security frameworks of IoT applications. Section 5 focuses on proposing a model for securing IoT applications and concludes the research.

2. CURRENT STATE OF ART OF IOT
The Internet of Things (IoT) is a promising worldview, which coordinates a substantial number of heterogeneous and unavoidable items with diff erent associating and figuring capacities, which are gone for providing different views around the physical world [1] [8].

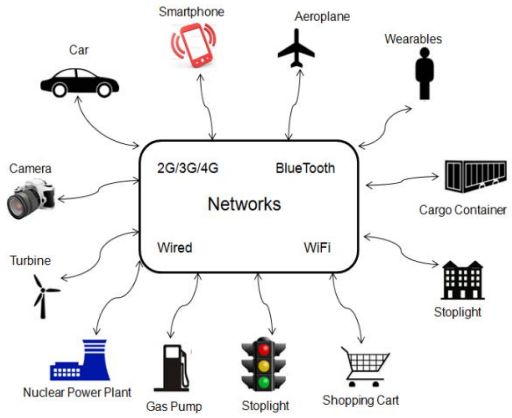

Fig. 1: Internet of Things (IoT) [4]

According to Figure 1, IoT applications are considered connected heterogeneous devices through communications gateways. It is normal that IoT innovation will make ready for momentous applications in a decent variety of territories, for example, medicinal services, security, observation, transportation, and industry. Additionally, it will have the capacity to coordinate advances; for example, propelled machine-to-machine (M to M) correspondence, autonomic systems administration, basic leadership, secrecy insurance and security, and distributed computing with cutting-edge identification and activation advances. In fact, IoT includes both static and dynamic objects of the physical world (physical things) and the data world (virtual world), which can be recognized and coordinated into correspondence systems. The basic highlights of IoT include:

(I) interconnectivity, (ii) things-related administrations, for example, security assurance and semantic consistency, (iii) heterogeneity, (iv) support of dynamic changes in the state and the quantity of gadgets, (v) tremendous scale [2,8 and 9].

2.1 Architecture of IoT
IoT applications are made up of a set of layers and each layer has a set of attributes and characteristics that work together to achieve a specific goal. A group of analysts and their work on the Internet have shown in [10-12] that they consist of three layers and have multiple names such as layers of perception, layers of the network, their work and a layer of the application itself, and each layer with security problems. The design and structure of the third layer of Internet objects were shown in Figure 2.

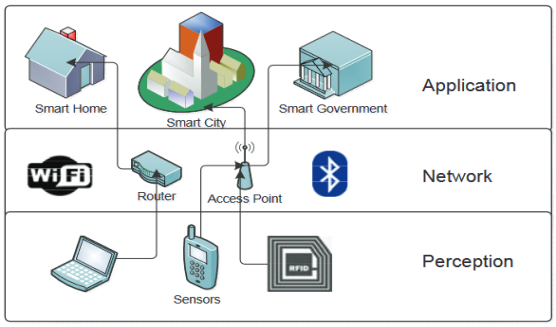

Fig. 2: Design and architecture of the third layer in IoT [5]

2.2 Characteristics of Internet of Things (IoT)

"The characteristics and features that characterize the Internet of Things". They have many characteristics that are characterized by the following properties:

- **Interconnected**: It encourages individuals to participate in gadget to gadget interconnection.
- **Smart Sensing:** The gadgets associated with IoT will have keen detecting abilities. For instance, utilization of movement sensors to turn lights on or off. The detecting innovation makes encounters that mirror a genuine familiarity with the physical world, individuals and articles.
- **Intelligence:** The IoT associated gadgets can have knowledge appended with them. For instance, Nest Learning Thermostats are Wi-Fi empowered.
- **Spare Energy:** IoT gadgets like Motion Sensor Light have in-fabricated movement finders which can turn the light on when it detects development. It can spare part of energy vitality from wastage and lift vitality collecting and productive usage of energy.
- **Communicating:** IoT associated gadgets have one of a kind ability to advise the present state to other associated gadgets in the encompassing area. It encourages better correspondence streams amongst humans and machines.

3. SECURITY CHALLENGES OF (IOT)

The security issue is the main focus of the Internet of Things (IoT) associated agents. The IoT application information can be close to home, venture, mechanical or customer yet put away information ought to be secured against robbery, altering and ensured in the travel and very still. For instance, an IoT application may stores streams and chronicled information of a person's wellbeing, shopping conduct, area, funds and amount of stock, business orders and so on. The IoT energizes another level of outsourcing; however, there are worries around benefit accessibility, adaptability, reaction time, value structure and protected innovation possession and so forth.

In the meantime, various difficulties are impeding the IoT. Regarding versatility, IoT applications that require huge quantities of gadgets are frequently difficult to execute as a result of the confinements on time, memory, preparing, and vitality limitations. For instance, estimation of everyday temperature varieties around the majority of the nation may require a large number of gadgets and result in an unmanageable measure of information. Moreover, the sent equipment in IoT regularly have diverse working qualities; for example, examining rates and blunder dispersions, then sensors and actuators parts of IoT are constantly exceptionally mind-boggling. These components compile to the running of the varied systems of IoT in which the information of IoT will be profoundly heterogeneous. Besides, it is costly to transmit immense volumes of crude information in the unpredictable and heterogeneous system, so the IoT requires information pressure and information combination to diminish the information volume. Thus, institutionalization of information handling mindfulness for future IoT is exceptionally wanted.

Security is a concern when information is processing through the Internet or even privacy systems and VPN burrows. The Government controls, for example, Health Insurance Portability and Accountability (HIPA) Act or confinements on transporting information crosswise over global fringes can be connected as wellbeing measures. The key IoT security undertakings ought to guarantee that appropriate application level assurances like Distributed Denial of Service (DDoS) assault relief are set up. It should likewise fuse measures to affirm the character of elements asking for access to any information including multi-factor confirmation [13] [14].

- **Information Privacy:** Smart TVs are gathering information about survey propensities and in some cases, they shaft listened in discussions back to a maker.
- **Information Security**: The Internet of Things (IoT) is enabling information to be exchanged consistently from observation gadgets to the Internet to empower live investigation. In any case, information security still remains a test here.
- **Insurance concerns:** The independent autos are including protection industry concerns. In any case, information will make it simpler to evaluate dangers and it gives a chance to new valuing models. For instance, protection premium tuning in light of wellbeing and driving information.
- **Absence of Common Standards:** There is not kidding absence of brought together standard for IoT and accomplishing an industry-wide acknowledgment of one bound together standard is an enormous test.
- **Technical Concerns:** Each IoT gadget can create a gigantic measure of information. It is a test to store, secure and break down. The system ought to have the capacity to deal with high volume and thickness of the gadgets. Additionally, it ought to be fit to distinguish and separate amongst allowed and rebel gadgets.
- **Social and Legal Concerns:** There is no instrument to address these social and lawful concerns [3]
  In addition, privacy-Preserving Protocols for Secure and Reliable Data Aggregation in IoT Enabled Smart Metering Systems" by (Samet Tonyali et al.) [17]. This paper handles protection issues raised by visit information accumulation of savvy metering frameworks. Current frameworks apply protection by deleting collected in-organize information (secure MPC) [15]. Be that as it may, both FHE and secure MPC are delivering overhead in IoT situations. In this manner, Samet Tonyali, et al. proposed another convention which uses FHE and secures MPC in Smart Grid (SG) Advanced

Metering Infrastructure (AMI) to lessen overheads while giving a practical protection safeguarding information conglomeration component.

Singh et al. [4] clarified the idea of the Internet of Things (IoT) its attributes, clarify security challenges, innovation selection patterns and recommends reference design for Ecommerce undertaking.

Jing et al. [18] proposed study focused on most of the security problems that threaten the applications of IoT as these applications rely heavily on the Internet. And through the three layers of the Internet of Things - the layer of observation and the layer of data transfer and work on it and the layer of the application itself. In this research, an emphasis was placed on solving the security problems of each layer on its own. "In addition to providing solutions through the paper to the problems of heterogeneity in detail by studying all the security issues related to the Internet of Things in general. At last, this paper thought about security issues amongst IoT and conventional systems and examines opening security issues of IoT".

Mahmoud et al. [5] displayed a study and examination of the concept of the IoT system, which builds on the basis of connecting the objects together, connects anything to anything else. As a result of the IoT architecture, there are three layers, layers of visualization and the network and application and on the basis of that must adopt a set of security standards that achieve real levels of security for each layer and to achieve a high level of security for Internet applications in general. Many IT professionals have worked to solve many security problems in the various Internet classes by implementing and implementing countermeasures and measures against these attacks and security risks. Through the research, all security standards, challenges and procedures were identified in order to provide complete protection.

4. CURRENT FRAMEWORKS AND ARCHITECTURE OF IOT SECURITY MECHANISM

TACIoT: A system that relies on more than one standard or factor is called a multi-core system and relies heavily on building trust for the Internet framework of things. The Internet of Things is working to build mechanisms and models specific to achieve high levels of security to meet security challenges. In the past years, a number of initiatives and works have been undertaken to build and design services and models within a specific vision. The vision has been built and designed within specific domains to meet a range of requirements, regardless of the nature of Internet applications. In this sense, the FP7IOT-A initiative builds on an interoperability system between the different applications of the Internet to create a global system of services under a common framework for a range of applications.

This system is a reference model called ARM. The system is based on the promotion of a common understanding and meaning of a high level of abstraction by describing the structural structure of Internet applications called IoT-A. Through this system, a number of additional initiatives emerged as the starting point for designing a unified security system such as BULTER, and the adoption of such systems on the basis of the identification of appropriate security and privacy mechanisms for Internet scenarios, which led to many of the privacy achieved for applications. Figure 3 illustrates the various functions of safety within this model.

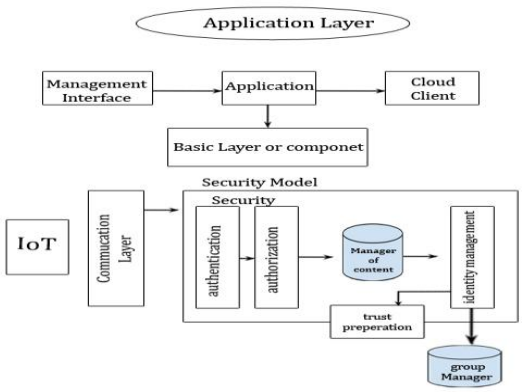

Fig. 3: Access Control for IoT

The infrastructure of Internet applications is supported by the design and development of specific mechanisms to deploy and build standard security solutions with the heterogeneous medical consideration of the system through which Internet applications are implemented.

The most important protocols that fully support the security infrastructure (CoAP) that protocol remains a standard transfer of discretion in Internet object scenarios. Although the CoAP protocol is similar to the same HTTP standards, most services can be achieved on all restricted devices and networks. It provides many security modes for protocols by connecting the security layer to the Datagram.

Most of the research and the scientific research community in recent times has received great attention in the application of access control mechanisms and control of the Internet of Things and began many efforts to appear in this direction. However, due to severe restrictions on Internet hardware resources, most of these proposals assume the use of a central entity on the Internet, responsible for security mechanisms and access control.

As a result of the lack of an appropriate Internet access control solution, the IETF Working Group for Authorization and Authorization of Restricted Environments (ACE) was recently created to create standardized authentication and licensing mechanisms that are deployed on devices and networks with limited resource constraints

5. ACCESS CONTROL FRAMEWORK FOR IOT DEVICES

Access control framework for IoT devices and their services, via security policies residing on resource-rich infrastructure nodes**.**

The created Oauth-IoT structure offers get to control systems for the IoT, by appropriately utilizing and fitting the generally utilized open benchmarks. The reference engineering grasps the accompanying segments:

1. Internet of Things network. It incorporates numerous obliged gadgets ready to detect the encompassing condition, secure information, (for example, temperature, stickiness, glow, and quickening) and convey them to a sink hub, additionally called organize organizer, through a low-power and short-go remote correspondence innovation. The sink hub is joined to the Gateway that goes about as a Resource Server and offers much usefulness.

2. Client. In accordance with the OAuth 2.0 approval structure, it is an outsider application willing to achieve assets having a place with an IoT arrange, for the asset proprietor. It would get to remote assets through OAuth 2.0 natives.

3. Gateway. It is a key hub of the proposed engineering that executes the OAuth 2.0 Resource Server and an interface between OAuth 2.0 and the IETF convention stack. For sure, it offers security functionalities (e.g. foundation of TLS station with the customer, verification, and access control), the following of accessible assets (through the asset revelation method), and other framework functionalities (e.g., information storing and freshness controls).

4. Authorization Server. It manages authorization mechanisms, as detailed by the OAuth 2.0 authorization frameworks.

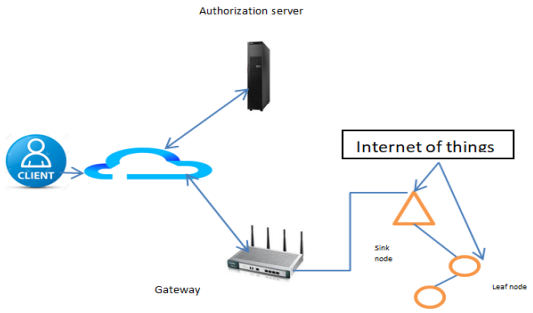

Fig. 4: The proposed architecture Oauth-IoT Framework

5.1 Use IoT Data Encryption

To protect the privacy of users and prevent IoT data breaches, encrypt the data at rest and in-transit between IoT devices and back-end systems by using standard cryptographic algorithms and fully-encrypted key lifecycle management processes to boost the overall security of user data and privacy.

5.2 Use Iot API Security Methods

Use IoT API Security methods not only to protect the integrity of the data movement between IoT devices, back-end systems, and applications using documented REST-based APIs, but also to ensure that only authorized devices, developers, and apps are communicating with APIs or detecting potential threats and attacks against specific APIs.

Table 1. Summary of different security mechanisms used for securing IoT applications

Methods	Advantages	Limitations	References
TACIoT: This model builds domains to meet a range of requirements	Understanding and meaning of a high level of abstraction by describing the structural structure of Internet applications called IoT-A. Through this system, a number of additional initiatives emerged as the starting point for designing a unified security system. TACIoT extends traditional access control systems by taking into account trust values which are based on reputation, quality of service	TACIoT should be implemented and evaluated in a real testbed for constrained and non-constrained IoT devices.	[9][10]
The CoAP protocol	It provides many security modes for protocols by connecting the security layer to the Datagram	Lack of an appropriate Internet access control solution.	[7][9][10]
Access control framework [Oauth-IoT]	It incorporates numerous obliged gadgets ready to detect the encompassing condition. In accordance with the OAuth 2.0 approval structure, it is an outsider application willing to achieve assets having a place with an IoT arrange, for the asset proprietor secure information.	OAuth 2.0 focuses only on client developer simplicity while providing specific authorization flows for web applications.	[4][5][9][10]

Use IoT Data Encryption	Protect the privacy of users and prevent IoT data breaches, encrypt the data at rest and in-transit between IoT devices.	Relying on cloud providers to secure your data.	[1][2][3]
IoT API Security Methods	Ensure that only authorized devices, developers, and apps are communicating with APIs or detecting potential threats and attacks against specific APIs.	Complexity of implementation.	[1][4][5]

6. CONCLUSION

The Internet is expected to incorporate advanced communication technologies, cloud computing, sensing and stimulation, paving the way for leading applications in a variety of areas, which will affect many aspects of people's lives and bring many amenities. However, because of the large number of connected devices that can be at risk, there are significant risks about "security, privacy and governance issues in the Internet." This paper has focused on security issues and challenges in the Internet of Things and presents some open challenges in this area and through research. In addition, many of the

problems related to the security aspect of IoT applications were discussed and some suggestions of the previous solutions were presented. Finally, a comparative study has been conducted through the research for trying to determine the highest levels of security for IoT applications. Along with the current proposed methods, it is important that further research should avoid and overcome the current limitations in IoT security methods in order to provide optimal security solutions.

7. ACKNOWLEDGMENT

This work is supported by the College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia and Swinburne University of Technology in Australia.

8. REFERENCES

[1] Nitti, M., Pilloni, V., Colistra, G., & Atzori, L. (2016). The virtual object as a major element of the internet of things: a survey. IEEE Communications Surveys & Tutorials, 18(2), 1228-1240.

[2] Bernabe, J. B., Ramos, J. L. H., & Gomez, A. F. S. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft Computing, 20(5), 1763-1779.

[3] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[4] Singh, S., & Singh, N. (2015). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In Green Computing and Internet of Things (ICGCIoT), International Conference on (pp. 1577-1581). IEEE.

[5] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In Internet Technology and Secured Transactions (ICITST), 10th International Conference for (pp. 336-341). IEEE.

[6] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks, 20, 2481-2501.

[7] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17, 2347-2376.

[8] Ashton, K. (2009). "That internet of things' thing," RFiD Journal, 22, 97-114.

[9] Atzori, L., Iera, A., Morabito, G. (2010). The internet of things: A survey. Computer networks, 54, 2787-2805.

[10] [M. Abomhara and G. M. Koien, (2014) "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.

[11] K. Zhao and L. Ge,2013 "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667.

[12] M. Leo, F. Battisti, M. Carli, and A. Neri, 2014. "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5.

[13] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar,2015 "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111.

[14] [R. Roman, P. Najera, and J. Lopez, 2011 "Securing the internet of things," Computer, vol. 44, 51-58.

[15] R. Roman, J. Zhou, and J. Lopez,2013. "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279.

[16] Romdhani, Imed & Abdmeziem, Riad & Tandjaoui, D. (2015). Architecting the Internet of Things: State of the Art.

[17] [Samet Tonyali, Kemal Akkaya, Nico Saputro, A. Selcuk Uluagac, Mehrdad Nojoumian, 2018. Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems. Future Generation Comp. Syst. 78: 547-557.

[18] Qi Jing, Athanasios V, Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qui,2014 "Security of the Internet of Things: perspectives and challenges", Springer, Wireless Networks, vol. 20, Iss.8, pp. 2481–2501.