Embedded IOT System: Software and Security Attacks

Muhammad Ayub Sabir, Muhammad Sheraz Arshad Malik, Fatima Ashraf and Rubab Rasheed

Abstract
Internet of the things is the latest trend in the Internet world with all its embedded systems and applications. It includes the wide variety of the smart devices that are sending the huge amount of data. The main challenge is when the IoT systems are connected with the internet, it is affected by the different attacks. The software stops its operational steps and badly affecting the normal working of the system.
These attacks also affected the application of IoT that is connected to the internet. IoT smart devices also threats the authentication and physical attacks. End to End communication nodes is disconnected when the system is attacked by the external or internal attack. While the connection with the internet it creates many challenges like integrity, stability issues. The traditional method is failed to create a secure barrier against these attacks. A security framework is required to handle all the things.
This paper investigates the new way to secure the system in an effect when the IoT devices integrate with the internet. Middleware security for the secure end to end communication between the sender and receiver and provide a shield against the vulnerable attacks. Introducing the core component that IoT Name Resolution Service (IoT- NRS).
Key words:
IoT, Middleware Security, Real-time operating system

1. Introduction

The first concept of the internet of the things implemented in the 1980's and gain a huge popularity in the 1990's. With the evaluation of the time, many recent developments have been concluded in the IoT and it includes many of the things like wireless sensors, embedded devices and contains microcontrollers that control the system. Over the past few decades, the volume of data has been produced as there's increasing demand in the internet of things (IoT) devices. Millions of the Internet of things devices have been connected to the internet and data is increasing day by day. The transmission rate of sending and receiving the data is also increasing. This generates the huge amount of data. Handling the huge amount of data is the most challenging task with the proper security and integrity.
Currently, IoT is present in almost every field and is playing a very major role in almost every activity. This is also using in the different professions like health, home automation, building structure management, transport systems, infrastructure management.
Embedded IOT systems are used to send the data and receive from one network to another network. It is based upon the microcontrollers and software that program according to the instructions. These embedded systems depend upon the Android-based system or Linux based. General purpose operating systems are also used. Vulnerable attacks upon the IOT system to steal the information. When the IoT is connected with the internet, it creates the integrity issue and authentication with the physical threats also arises.
Real-time operating system (RTOS) is also used as they are more efficient and flexible to maintain the high performance. As extensive software can easily be run on the real-time operating system. Connecting many of the IOT systems with the internet arises many challenges.
A huge number of IoT devices are connected to the internet and it's increasing its volume day by day with an increment in the population. It would be nearly 26 billion in 2020. While the connection with the internet it creates many challenges like integrity, stability issues. To address this problem many solutions many been concluded but they are failed to secure the system as they cracked the system and take out the private information. Even though the data traveling hackers create the barriers and packets of the data is missed through the data travel. This volatile the privacy and security issues.
A breach of the internet and take out the personal information creates many physical and general threats as they leakage the personal information of the common people which intend to create many huge problems. Even they spread the virus in the system that and data is a big threat.
The connectivity of the IoT and the Internet also supports the physical attacks. Low-end Internet of Things is not capable of performing in an efficient manner due to their constrained source to integrate the things.
The traditional architecture of the IoT creates the fundamental issues of server failure and mobility issue. To fill this gap a new approach has been proposed that provides the security to the IoT networks and the application of the IoT. The Middleware layer provides the security frame where the authentication and attacks can be avoided. Basically, middleware security consists of three layers that are local service gateway, aggregator and IoT server. It supports the different functionalities, system management takes, and the data generated by the IoT devices.
This paper investigates that how securely we can integrate the Internet and IoT embedded system through which the systems can be secured, and protocols have been introduced to avoid the physical attacks. Through the investigation, vulnerability measures have been concluded in the existing

Manuscript received August 5, 2018
Manuscript revised August 20, 2018

IoT systems. A secure IoT middleware framework has been introduced to support the systems and provide the security in the most efficient way. End-to-End barriers have been created so that no vulnerable attack can be avoided with the great efficiency and effectiveness. Introducing the core component that IoT Name Resolution Service (IoT- NRS)

2. Literature Review

IoT is playing very important in our daily life and has a big impact in the near future. As it generates the instant solutions to the different problems. There is a massive increase in the smart devices and there are generating a huge amount of data on the daily basis. IoT is the huge network that consists of physical devices and connections. The software sensors and electronic signals make them unable to exchange the information from one place to another. This builds the communication system between the different devices.

This communication network generates the data from the different devices. As IoT generates the huge volume of data and Big Data manages that data to produce the productive results. But when the IoT systems are connected with internet this creates a huge mass to supports the different communication layer all together and security is the vital element in the IoT systems.

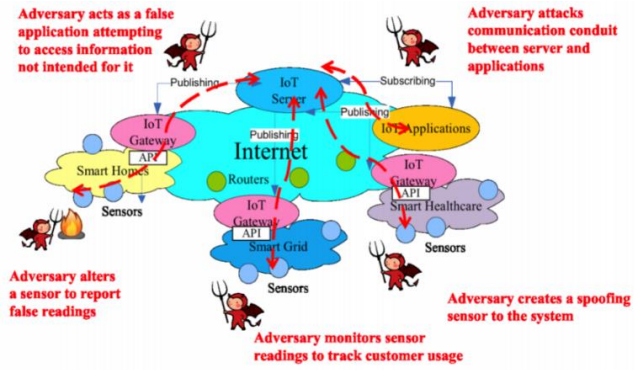

Fig. 1 Potential Threats of IoT

The vulnerable attacks keep the system held and the information is easily being stealing at this stage. This is the most challenging part as the security of the personal credentials and personal information is very necessary to be protected from the hackers and other viral attacks.

IoT consists of different layers and each of them is connected through a communication channel that provide end to end connectivity. And each layer is sending and receiving the huge amount of data and this end to end communication path make it easy to transfer the huge amount of data even in Nano seconds.

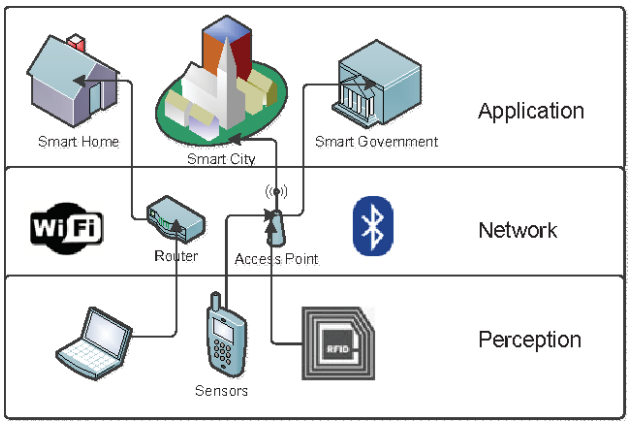

Fig. 2 Three Layer IoT Architecture

Confidentiality is the key element in this three-layer architecture, but it failed to support the system when it is targeted by the external and internal attacks. This is a big challenge and unable to solve the traditional methods or manual implementations.

IoT generates the unstructured data and the volume it generates is also very critical. To dig out a specific information it can be a tedious task or nearly impossible to handle. Moreover, continuous operational steps are required to handle the data generated by the zillions of devices. To get the insight from the semi-structured and unstructured format of data, the data must be analyzed in an appropriate way and the low-performance area have to detected in the most efficient manner. Where the operational process can be simulated, and the efficiency of the system is remaining even it is attacked by some heavy virus. The system should be encrypted in an efficient manner where the data and its application can perform the processing in an effective way. The cluster of information is stored and analyzed. The updating process is being occurred so that only the formatted data can keep that delivery of some valuable information and can be protected from any time of attacks and keep the communication smooth.

3. Methodology and Design

Through the survey it is concluded that current IoT systems doesn't support the applications and infrastructure doesn't provide the security for the smooth communication. The traditional approach has many fundamental issues and unable to provide the secure channel.

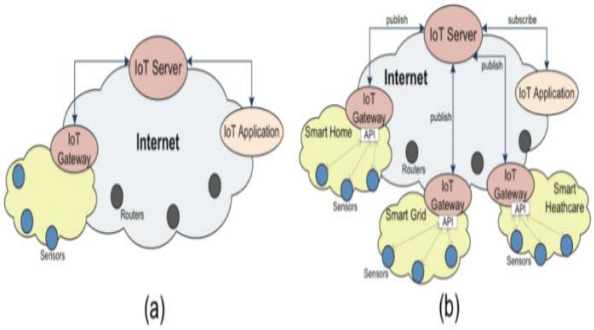

Fig. 3 Legacy of Internet of Things and Overlay based IoT architecture

Fig a. explains a large number of legacy of the Internet of things that are independent to perform the different activities. But it introduces the problem of service level interaction during the communication and inter-operability operations that limits the real benefits of IoT devices and systems. Fig b. explains the overlay based IoT architecture forms of networks that supports the different things.

Different deployments can be occurred, but it does not support the system and several weaknesses are evaluated during the runtime integrity. If the central server of the IoT is failed the whole network will be failed badly and data is gone out the way. Moreover, it doesn't support the internet mobility and a protection layer to support the physical attacks.

By overviewing the different issues, the solution has been proposed to overcome this problem and it include the middleware security, key management protocol.

Middleware Security

By overviewing the different issues, the solution has been proposed to overcome this problem and it includes the middleware layer, the middleware layer includes the core component that is IoT-Name Resolution Service. IoT-NRS works in the most efficient way when the new devices join the local system, it acted as the authority to verify the new device and registered it with unique ID.

A new concept has been introduced that fills the gap in the previous research and proposed methods. It is one of the most essential elements that is IoT middleware to handle the data distribution and system management with a secure protection to communicate within the internet integrity. Basically, middleware security consists of three layers that are local service gateway, aggregator and IoT server. It supports the different functionalities, system management takes, and the data generated by the IoT devices.

It provides the protection to be both structured and unstructured data. It provides the separation of the IoT systems and software with he is underlying networks that exist in the system. Middleware security is independent of the underlying networks and other infrastructure devices systems that exist in the system. It provides the secure encryption in the different communication systems.

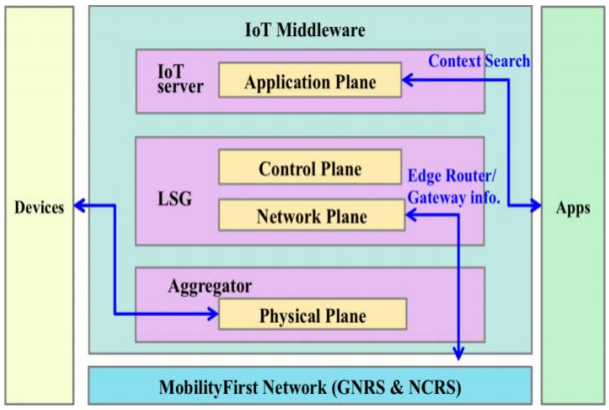

Fig. 4 IoT Middleware

Mobility First Network infrastructure provide many solutions that is facing by the IoT devices. It provides the stability and integrity while connecting with the internet. It provides end to end support where the different communication networks take place.

It introduces the new protocol and replace the TCP/IP. The new protocols are GNRS and NCRS stands for Global Name Resolution Service and Name Certificate and Resolution Service.

Name Resolution Service

Name Resolution Service to provide the authority within the network and identifies the devices and software within the local system. Different execution of the task can have verified, and attacks can be scanned thoroughly. System security within the network can be evaluated. The analyzed results can be evaluated for the research gaps in the traditional approach of IoT security and proposed solution are evaluated before the real-world simulation.

IoT Name Resolution Service is considered as one of the most simplified service in the network that provide the different stability, inter digit with in the communication network and provide the identifiers as well. It stabilized the long-term management key that provide the related identifiers to secure the network.

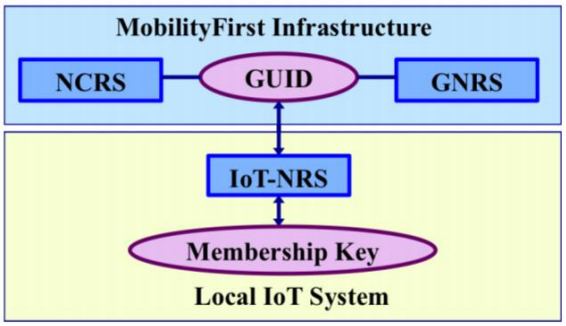

Fig. 5 Name Resolution Frame Work

Name Resolution Service provide the GUID service assignment that works together to assign the network objects, different IoT systems and network service within the internet connectivity. It developed the different relationship with in the network that is one-to-one, one-to-many and many-to-many. The membership key act as the authority with in the network and identifies the devices and software with in the local system. It provides as the security to handle the different execution of the tasks. It also guarantees the different system security with in the network. NRS also performs the verification and revocation tasks.

4. Conclusion

Embedded IoT systems are widely using all over the world and generating a lot of data. But this data required some security as the most private that is been there in the IoT systems. Different operations are performing on daily basis and processing of the raw data is been occurred to generate the useful data that can be used for the different purpose. When the IoT devices are being connected with the internet this is creating the huge mess and challenges to deal up the things all together. Traditional methods are badly failed to provide the security. This paper investigates the new ways to provide the security when the IoT systems are connected with the internet. A middleware is introduced that provide the extra layer of security. Name Resolution Service is being deployed to manage the identifiers and other functionalities within the network framework.

References

[1] Marimuthu, P, Rajkumar, B., Jayavardhana, G., Slaven, M., *Internet of Things (IoT): A vision architectural elements and future direction*, [online] Available: http://www.elsevier.com/locate/fgcs.
[2] Eric, Brown, (13 September 2016). "Who Needs the Internet of Things?". Linux.com.
[3] Ovidiu; Friess, Vermesan, Peter (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers.
[4] "Internet of Things (IoT)". gatewaytechnolabs.com.
[5] http://www.sas.com/en_us/insights/big-data/internet-of-things.html
[6] http://www.tutorialspoint.com/articles/how-iot-impacts-big-data
[7] Friedemann; Mattern, Christian, Floerkemeier, (2010). "From the Internet of Computer to the Internet of Things"
[8] Ashton (22 June 2009). "That 'Internet of Things' Thing".
[9] Commission of the European Communities (18 June 2009). "Internet of Things — An action plan for Europe". COM(2009) 278 final.
[10] Li, H. Jing, J.; (2012). "Research on the Relevant Standards of Internet of Things". In Zhang, X : Wang, Y.;. Internet of Things: International Workshop, IOT 2012. Springer. pp. 627–32.
[11] Iera, A.; Morabito, Ashton, K. That 'Internet of Things' Thing. RFID J. 2009, 22, 97–114. 2. Atzori, L.; G. The Internet of Things: A Survey. Comput. Netw. 2010, 54, 2787–2805.
[12] Giusto, D.; Morabito, G.; Lera, A.; Atzori, L. The Internet of Things; Springer: New York City, NY, USA, 2010.
[13] Herbert, John; O'Donoghue (1 October 2012). "Data Management Within mHealth Environments: Patient Sensors, Mobile Devices, and Databases". Journal of Data and Information Quality.
[14] Strategic Business (Firm). Six Technologies with Potential Impacts on US Interests out to 2025; Technical Report; The National Intelligence Council: Washington, DC, USA, 2008.
[15] Trade Commission. Internet of Things—Privacy and Security in a Connected World; FTC: Seattle, WA, USA, 2013.
[16] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020; Gartner Inc.: Stamford, CT, USA, 2013.
[17] MobilityFirst Future Internet Architecture. Available online: http://mobilityfirst.winlab.rutgers.edu/ (accessed on 19 June 2017).
[18] ; Hauswirth, M.; Aberer, K. Salehi, A. Infrastructure for Data Processing in Large-scale Interconnected Sensor Networks. In Proceedings of the IEEE International Conference on Mobile Data Management, Mannheim, Germany, 7–11 May 2007; pp. 198–205.
[19] Tsiatsis, V.; Blazquez, A.; Vandikas, K. Performance Evaluation of OpenID Connect for an IoT Information Marketplace. In Proceedings of the 81st IEEE Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–6.
[20] Abyi Biru, Roberto Minerva, and Domenico Rotondi. IEEE: Towards a definition of the Internet of Things (IoT). http://iot.ieee.org/, May 2015. Last accessed December 09, 2016.