ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 4, pp: (28-33), Month: October - December 2016, Available at: www.researchpublish.com

A Study on Highly Secured Transparent User Interface for IoT Appliances

Faustina Jeroma Anto Morais

Masters in Computing and Info Sciences, School of Computing, University of North Florida

Abstract: **The Internet of Things (IoT) refers to the network of physical objects and things connected to the internet. These objects will be embedded with electronics, software, sensors and network connectivity through which they collect and exchange data. IoT is the major growing technology as the application such as monitoring and home automation are used widely. Trustworthiness is one of the main issue with all the IoT appliances. This paper discusses about the enhancement of security system and trustworthiness by providing a virtual reality user interface with which they can check the end to end connectivity. The outcome will be the transparent middleware which shows the end to end virtual connectivity. The system can be used by the end users to operate their daily used domestic IoT applications.**

Keywords: **Internet of Things, Virtual user interface, information security.**

1. INTRODUCTION

Internet of Things (IoT) is built based on the internet and wireless network which are more liable to be intruded. From the perspective of informational and networking security, as a heterogeneous multi-network of the converged network, the Internet of Things has existence of the same security issue as the sensor networks, mobile communication network and the Internet, as well as their specificity, such as privacy protection, heterogeneous network authentication and access control, information storage and management. The development of IoT is based on information security and network security. Therefore security concern should be put first even before its development.

The security analysis should be still enhanced to make the system safe and secure. The paper briefly analyses about the security and trustworthiness of IoT applications. It deals with the technology to design a virtual reality user interface through which the user can control the IoT home appliances with transparent middleware such that the end to end connection from mobile to the device is shown virtually. Trustworthiness in the system is that the user can check the node connectivity from their mobile devices to the IoT devices such as the temperature controller, motion detectors and other security applications which are used in day-to-day life.

As it is transparent it is likely to think that it itself paves way for more intrusion, but not the entire middleware system will be transparent, it is just the node connections are shown so that they knew what is happening before the operations are performed simply instead on ON/OFF with their mobile devices. The study is because the security on data over the internet has no complete solution till date which is more important. This paper discusses, which method can be used, whether it is suitable or not, and also some evaluation methods to check the effectiveness of the methods. The 3D visual representation is what expected and let us see whether it is achieved and how secured it is compared to the existing systems.

2. RESEARCH QUESTION AND HYPOTHESIS

In the process of development of Internet of Things, the current or next-generation Internet will be the Internet of Internet of Things core carrier transport layer [7], most of the information will be transmitted over the Internet with the three dimension of any time, any place, any matter. Encountered in the Internet and Distributed Denial of Service attack (DDoS) still exists, so we need better preventive measures and disaster recovery mechanisms.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 4, pp: (28-33), Month: October - December 2016, Available at: www.researchpublish.com

There were no transparency in the middleware till date for IoT devices. The users are allowed only to operate the IoT applications through their mobile and are unaware of how it is connected[2].

With these use of the middleware, Is the security achieved? Is there a total security that no device can be hacked? How secure the nodes and information are?

Perceived safety of the nodes: A large number of perception nodes, and spread over a large area, the lack of effective monitoring of people, the attacker can easily access to these devices, thereby causing damage to them, even through the local hardware and software replacement for the machine operation.

Insight and Theoretical Contribution:

In IoT application, the network is intruded by the attackers only in the middleware which is invisible to the user. It happens due to the lack of effective monitoring. If there is a system designed with transparent user interface with all the functionalities included virtually and if it can be monitored by the user itself, the system can be more secured. It is likely to think that the transparency are more exposed for the intrusion to happen, but it is just the virtual space to show the node connection. Mostly, only with the node detection, the intruders used to hack the devices. In this paper , various attacks are considered as in [1] for which algorithms are imposed to reduce the detection of neighbor nodes in the network. With the secured and good interface environment, trustworthiness of user will be increased.

It is difficult to design a common security scheme, and we should take different preventive measures for different network performance and network demand but a common user interface can be designed to view the connection established. Network transport layer security mechanisms includes end to end confidentiality and the confidentiality of node to node.

Security risks in wireless sensor networks is the network deployment area and the open broadcast nature of wireless networks, attackers often take advantage of these two features, by blocking the normal operation of the network nodes, and thus undermine the operation of the sensor network, reducing the availability of the network. Hence to resolve this the nodes and connection can be made transparent which reduces the security risks and protects user data[5].

System:

In this section, the proposed virtual user interface for the middleware design is described along with the ways on how applications interact with the middleware to dynamically load the user interface when a device is plugged into the middleware. Figure 1 shows the overall architecture of the Internet of Things in the global environment.

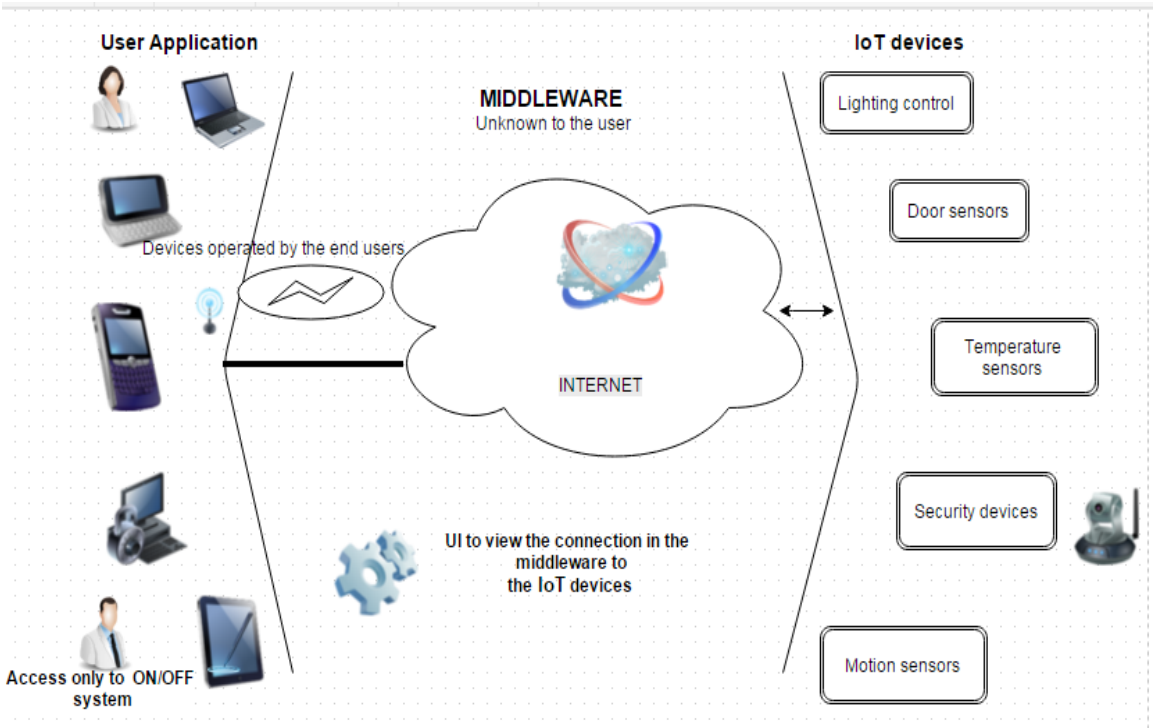

Figure 1. Overall architecture of IoT

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 4, pp: (28-33), Month: October - December 2016, Available at: www.researchpublish.com

IoT is a three layered architectures which involves the end user application, transport layer and the sensor layer. Figure 2 shows the layered architecture of the proposed system [7]. The transport layer is the middleware which will be the virtual space for the user to operate IoT devices and checks the connectivity of the sensors nodes so that they knew that there is no intrusion. Though the virtual space for the middleware does not include the exact operation of the connections of internal nodes, it can depict only the nodes which is connected from the end device to the sensors such that the intruders cannot make use of the transparency for further attacks.

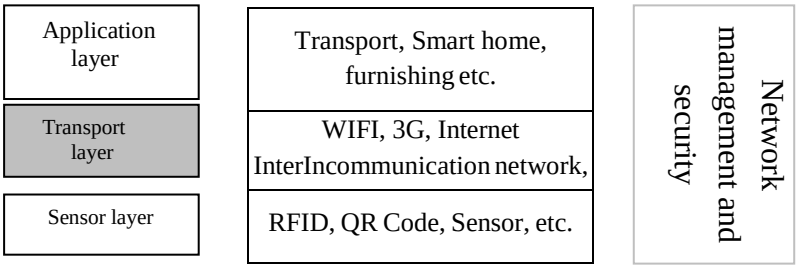

Figure 2. Layered architecture of Internet of Things

The virtual space operated by the end users can be designed in a three-dimensional interface as in Figure 3, such that the appropriate connection can be visually presented in a easy way which increases their trust on the system that it is safe and secure. Furthermore, the transport layer middleware is not completely transparent but it is only the virtual space to monitor the connection. Other than simply ON/OFF, the working of the system till the end connection are visually shown. It means that users can directly participate in what is happening in the scene they are immerged in. They can walk through the scene and behave in the logic of virtual reality. This scene presentation comprises all virtual technology nodes that can be completed by necessary information details. The movement between these nodes is subject to user's control or it can be pre-defined in advance. The method used for this virtual visualization is 'colliery dynamic imaging' which is the 3D virtual image provision.

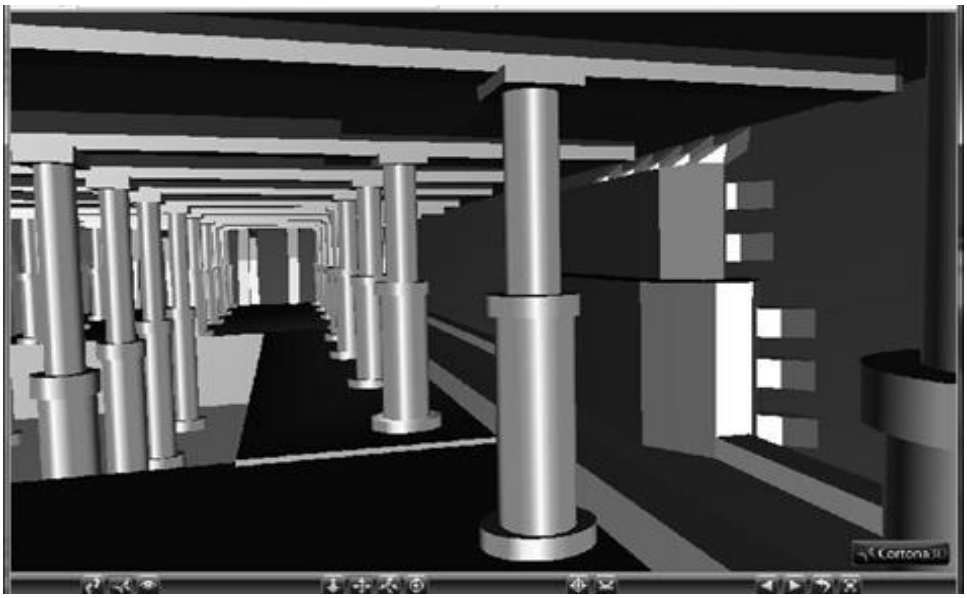

Figure 3. Virtual technology UI for IoT

3. RELATED WORK

Li-Qing Guo et al. [2] explains the bridge between the physical and virtual world in IoT. For IoT application developers, it is important to have a mechanism that can provide a uniform accessible interface, called middleware, which hides technical details of accessing hardware devices from application developers and helps them to concentrate their focus on the software portion of the IoT applications. To deal with this issue, they proposed a middleware architecture that is designed based on software engineering point of view to assist developers with an easier way to establish communication links between devices and their applications.

Takayuki Suyama et al. [3] provides a study on the architectural development of virtual machine (VM) for the sensor nodes. The speed of information technology development is ever increasing. The appropriate information can be easily provided for and often it can be visually presented. The paper introduces the sensor network system for VM and its use cases. Usually, both Java Virtual Machine (JVM) and Virtual Execution System (VES) for Common Intermediate Language (CIL) are the two most popular process virtual machines used on personal computers. In this paper, they denoted that an implementation of VES as CIL. Each sensor node in the sensor this proposed network has the CIL program on our implemented virtual machine. This sensor node obtains the data from each sensor by the CIL program. This virtual machine is designed to monitor the connection between the nodes and thus transparent to the user.

Ilker Onat and Ali Miri [6] discussed various attacks caused in the wireless sensors by the intruders. In many attacks against sensor networks, the first step for an attacker is to establish itself as a legitimate node within the network. Furthermore, they explained that to make a sensor node capable of detecting an intruder a simple dynamic statistical model of the neighboring nodes is built in conjunction with a low-complexity detection algorithm by monitoring received packet power levels and arrival rates. These algorithms though implemented, it cannot be monitored much if it is not transparent to the users. With these techniques involved, the detection of nodes can be reduced and thus with the virtual user interface the visibility and the security can be achieved. The first Intrusion Detection (ID) based security scheme for MANETs was introduced in [8] along with a general overview of requirements and architectural differences between ID systems for wireline networks and MANETs.

This transparent middleware solution, as in the works mentioned afore, was designed from software user interface point of view, helps IoT application developers to simplify the monitoring process. From establishing communication between the device and the application via the virtual interface, there increases trust which inturn increases the business value more on daily used domestic IoT application [4].

4. METHOD

The transparent interface of the middleware are more likely for attacks by the intruders. Here, as the entire connection are not made transparent but only the node connection where always the intrusion happens. In order to prevent powerful intruders disrupting network operations, specific properties of sensor networks are to be determined. To check the intrusion, cooperative solution which refers to the attack confirmation and collective action of neighboring nodes against intruders can be used.

• Nodes know what to expect from other nodes, particularly from their neighbors. They detect and report anomalies to each other. The essential property of sensor networks that allows for intelligent node decisions is the long term operation of the network with relatively stable neighborhood information for each node.

• Nodes share the unexpected behavior of their neighbor with other nodes. This provides confirmation and common action against the attacker(s).

Also, the detection and containment of an intruder using node cooperation has to be checked.

Detecting nodes may also propagate this information to neighbors that are not yet aware of the intruder. So, the cooperative containment solutions has to be designed which is the implementation of a node-based statistics gathering and analyzing algorithm.

The anomaly detection algorithm here are executed at each node separately for security of the nodes so that it is not easily detected and intruded in the transparent interface. The virtual reality (VR) is considered as the computer-assisted presentation of information which is implemented here to image the node connection in the network. Other than the algorithm, the main research method used is 'colliery dynamic imaging' which is the virtual image provision for any part of a colliery environment characterized by attributes specified. The movement between the nodes in the connection between IoT device and internet are shown virtually. It is as simple as using mobile which doesn't need any user training to operate.

5. EVALUATION PLAN

In the colliery dynamic imaging, virtual imaging is processed with the attributes specified such as Object Naming Service (ONS) query and RFID. For information distributed in internet, the usage of ONS plays a vital role. Sequence of bits denoting an Electronic Product Code (EPC) is read and send to a local server which is converted into URI Form (Uniform Resource Identifier). It is the input to the local ONS resolver which converts URI into domain name and issues a DNS query for NAPTR (Naming Authority PoinTeR) records for that domain. DNS creates correct URL through which the connection gets established.

EPC > local server > URI > local ONS resolver > URI > domain name > DNS query > URL

Measures:

The packet drop in each node in these process noted by pinging each node and the effectiveness is calculated. The anomaly detection algorithm includes training and testing. In the training stage, a set of feature vectors from a legitimate user is used to establish a profile of the user. ie, the connection is tested in a closed network (not liable to intruders) and the packet received/ dropped is noted. In the testing stage, the detector compares a new vector against the profile, and produces a detection score that indicates whether the new vector is similar to the profile or different from the profile. The procedure by which this score is calculated depends on the detector.

To transform these sets of detection scores of both legitimate users and impostors into aggregate measures of detection performance, the false-rejection rate (FRR) and false-acceptance rate (FAR) is computed. With these FAR and FRR between the nodes, the equal-error rate (EER) is calculated and ROC curve is plotted to check the effectiveness.

This study about the transparency in middleware and designing an user interface to control the IoT devices, interprets the security enhancement in IoT operation which is liable to more attacks.

6. ANTICIPATED FINDINGS AND CONTRIBUTIONS

Internet of Things characteristics faces not only the traditional mobile communication network security issues but also some special security issues different from existing issues in the network. This is due to the lack of effective monitoring and management.

IoT devices identify some local node safety issues. Since some applications of it can accomplish and replace complex, dangerous and mechanical work, so the machine equipment are deployed in unattended outdoor scene, which paves way for the attacker to access these facilities and replace the parts of equipment and chip implanted Trojan horses, the consequences is unimaginable. These things will be designed and implemented well in the future, must set up early warning systems with the noticeable user interface to view the connections happening inside the network.

In home IoT appliances, sensor nodes usually have single function as temperature measurement and carry less energy, making their have not complex monitoring and lacking of defense capacity. But the sensor network varieties form temperature measurement to garage door control, form road navigation to precise positioning, which have no specific criteria for the data transmission and the message signals. So we cannot provide a standardized security system.

In this proposed transparency in node connection, the packet drop and ROC curve which are calculated interior but only the 3D virtual picture is made to view by the user who may be novice. Even though the security is not met to maximum accuracy, network is made secured better than with the middleware in which the user has no idea about the connection and control of IoT devices.

7. CONCLUSIONS

As we all know, the future world will be smart enough with all automation starting from the food, daily activities till industries. The smart world typically relies on cloud computing and Internet of Things. Along with the internet, the 3D visualization will rule the world. The more the technology, the more the users as it is easy to use. Only because the users are ready to use whatever it is automated without even knowing the security issues, does not mean we should exploit that and ignore the security implications. It should be associated with infrastructure and security aspects.

This paper analyzes existing research problems and challenges and provides opportunities for future research work in this area. In conclusion, it is believed that this study work may provide an important contribution to the research community, by documenting the current security status of this very dynamic area of research and motivating researchers interested in developing new schemes to address security in the context of the Internet of Things.

REFERENCES

[1] Md. Mahmud Hossain, Maziar Fotouhi and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", in 2015 IEEE World Congress on Services, July 2015, pp 21-28

[2] Li-Qing Guo, Da-You Huang and Kuo-Hsun Hsu, "A study of middleware for pluggable UI in IoT-enabled environment", in 2014 IEEE 11th International Conference on e-Business Engineering, Nov 2014, pp 326-330.

[3] Takayuki Suyama , Yasue Kishino and Futoshi Naya, " Abstracting IoT Devices using Virtual Machine for Wireless Sensor Nodes", in 2014 IEEE World Forum on Internet of Things (WF-IoT), Mar 2014, pp 367-368.

[4] Fei Fan and G Zhao Zhou, "Analysis of the business model innovation of the technology of internet of things in postal logistics", in 2011 IEEE 18th International Conference on Industrial Engineering and Engineering Management, Sept 2011, pp 532-536.

[5] Ricardo Neisse, Igor Nai Fovino and Gianmarco Baldini, "A Model-based Security Toolkit for the Internet of Things", in 2014 9th International Conference on Availability, Reliability and Security, Sept 2014, pp 78-87.

[6] Ilker Onat and Ali Miri, "An Intrusion Detection System for Wireless Sensor Networks", in Wireless and Mobile Computing, Networking And Communications IEEE International Conference, Aug 2005, pp 253-259.

[7] Xu Xingmei, Zhou Jing and Wang He, "Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things", in 2013 3rd International Conference on Computer Science and Network Technology, Oct 2013, pp 825-828.

[8] Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks”, Mobile Computing and Networking, Aug 2000, pp. 275–283.