Advances and Applications in Mathematical Sciences
Volume 19, Issue 6, April 2020, Pages 543-549

SECURITY CONCERNS OF SMART HOMES AND ITS SOLUTIONS

GURPREET SINGH, KAPIL MEHTA and HIMANSHU SINGLA

Department of Computer Science and Engineering
Chandigarh College of Engineering
Landran, Mohali, India

Abstract

This Paper presents the security issues with the internet of things. IoT is new era were physical objects connected through a network were they can share the date. There are numerous applications in IoT like Wearables, Smart Cities, Smart Homes, Telehealth and many more. The main challenges that IoT facing is Security. The objective is how to make a secure network were physical objects send the data without the rapidly that company's don't emphasize on security issue with IoT we have to do work on the security of new products that will be coming in IoT market. In this paper, our concern is that how to make a secure home automation system for ensuring confidentiality and security by using the various types of standard encryption techniques. This paper is a holistic overview of the available solutions for a home smart devices security.

I. Introduction

As we know there is billion of IoT devices exist in today's world. There is easy security thread to this Billion of devices. Home automation make our lives easy but also due to lack of security there is always been thread to our personal data. As there are numerous unsecured devices connecting to the Internet day by day and Security experts are warning about the potential risk.

Most of the IoT products work in the wireless environment. Services can be said to be the requirements related to security provided over the home network environment. Smart Devices can be accessed by the attacker or invader in the network. There are various requirements for a smart home that includes safety, integrity, availability and authentication. The overall

2010 Mathematics Subject Classification: 74M05.
Keywords: Smart Home, Security, Envirnment, IoT.
Received 21 November 2019; Accepted 3 January 2020

idea is to make connection with devices at any time anywhere by anyone using the same path or services.

To make the efficient communication and passing of information amongst themselves, Machines can learn by easily recognizable to get intelligence to allow contexts. This can be possible with the cloud system presence and introduction. Cloud System is the possibility that can help to access or fetch data from the cloud. To handle limited capacity, transition is allowed from the Internet to IPv6 [3].

Home Security Objectives

In this paper, commonly Six goals have been considered [5] for smart home security as listed below:

- **Data Confidentiality:** Data can be accessed by the authorized parties.

- **Data Integrity:** It assures the security of homes by using a special secure mechanism like Digital Signature, Hashed Structure so that none can affect the security feature. There may be a chance that Attacker or Intruder tries to attack or access the things but that can fall the security of overall network. Interference by the attacker spreads the malicious code to affect the things, so it is necessary to use safety and security features so that Integrity of the network should be maintained.

- **Availability:** It allows to access the data over the wireless network offline and online. A Smart device user sends the request and received by the network and responding can be done to and fro. Fabrication and modification of information can be also done. Data can be of any type Fictional or Non-Fictional. Fictional data can cause inconvenience and malfunction of smart devices. Deterioration can lead to overloading of services that can generate financial loss from a rise in electrical rate that can affect lives. It is necessary to restrict functions from the outside parties for the functional access [7] [8].

- **Authenticity:** Several devices exist those security is not considered. If intruder or attacker access or attacks a malicious code in a smart device, then it is possible that smart home equipments will not work and the device will be of fake functions e.g; DOS, DDoS etc. On the other hand, if an intruder interrupts an updated module as a normal module then it degrade the function of the normal module and thereby availableness will be deteriorated.

So, authentication is highly needed for a smart device. Certificate will be used for the authentication [6] [9].

• **Authorization:** Access of right entity at the right place for the access control purpose [11].

• **Non-repudiation:** It means that undeniable proof will be used for the truthfulness verification of any claim of an entity.

II. Security Threats

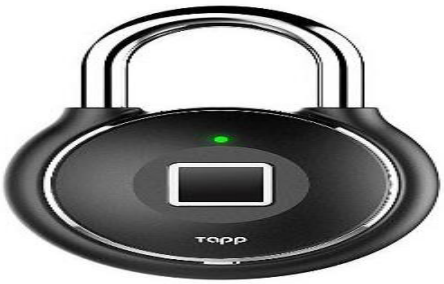
With the competition between smart devices on the rise of many manufacturers in a rush to get their products on the market and may not even provide sufficient built in security from cyber threats. This then becomes a easy access for hackers to either expose personal data or even launch an attack on much larger scale. the insecure implementation of IoT were a large number of internet of thing devices including various home appliances like Smart TV, Air Fryer, Refrigerators, Washing Machine, Security Cameras, Microwaves, smart bulbs, smart watches, are being hacked several times and can be used in cyber-attacks or wars as weapons.

• **IOT SMART TV**

Major portion of the smart tv can be hacked using broadcasting signals remotely.

The biggest malware based on IoT like Mirai-emerged in the last year and caused internet outage by launching massive DDoS attacks against DynDS provider-used for the hacking of connected devices in an easy way.

• IOT Smartlocks



• **Tapplock Smart Fingerprint Padlocks**

Tapplock can be said as an "unbreakable" smart lock. But it is probable that it's easy to crack the lock in around 10 seconds open with some bolt cutters. In the more quick fashion, that can be hacked using Android app in just 2 seconds. There are many IoT products, like this in which security build are very cheap.

III. Threat Awareness for Smart Home Owners

Security for homes can start with the awareness. If People get aware about the security feature then that can secure the whole home network:

• It is being assured that router software of home is always updated that must contain important fixes of security for vulnerabilities found in current software's version.

• It is being assured that firewall installed in the network should be initiative line of defense against intrusion of the network.

• Installation of latest system software on connected devices should be there. Security issues should be focused in the system update.

These are the things we should check before buying any IoT product. There is a list of six recommended security features that manufacturers can build into IoT devices, and that consumers can look for on a device's box or online description while shopping.

• **Device Identification:** The IoT device should have a way to identify itself, such as a serial number and/or a unique address used when connecting to networks.

• **Device Configuration:** Similarly, an authorized user should be able to change the device's software and firmware configuration. For example, many IoT devices have a way to change their functionality or manage security features.

• **Data privacy:** Data that is protected should be clear so that sending over the network and storage should be transparent. For Example, several devices use encryption technique to retrieve the data stored in the device.

• **Limited access:** Limit access should be there for network interfaces e.g.; supporting software and Device should gather & authenticate the user identity and attempt to access through secure credentials like username and password.

• **Software & Firmware Update:** A device's software and firmware should be updatable using a secure and configurable mechanism. For example, some IoT devices receive automatic updates from the manufacturer, requiring little to no work from the user.

• **Cyber Security Event Logging:** IoT devices should log cybersecurity events and make the logs accessible to the owner or manufacturer. These logs can help users and developers identify vulnerabilities in devices to secure or fix them.

IV. Discussion

We know that internet of things is future but who want live in a future that is not secure or safe so we have to work on the security of future IoT products. The main problem related to security issues on IoT devices is that we cannot change the default passwords by the user at their end. So, a control is required it is required to control the device in a DDoS attack. Various software are used for device control is a malware package named Mirai. Various software and hardware mechanism are available that quickly destroy the Internet. So, it is required to keep safe during communication or passage of information.

V. Conclusion & Future Scope

There are many challenging issues need to be address to be united to get the realistic secure version of IoT. The main issue is interoperability between connected devices and the smartness degree by enabling the autonomous behavior that guarantees security and privacy of the users and their data [3].

"Securing devices is a group effort," Fagan said. "The manufacturer has to supply options and software updates, and the user has to apply them. Both sides have roles to play." However, IoT will pose several problems related to efficient utilization of resources in low battery constrained objects.

Various Inventors & Experts on the Internet of Things are planning and coming together that includes groups, peers, associations, manufacturers etc. so that they can work form smarter authentication and security. Such solutions are the security measures to be taken care of for the better security.

There should be manufacturer security settings followed by IoT Industry standards born from the association of network engineers, developers manufacturers and solution providers.

We are moving so quickly and working on innovative solutions so that newer information security can be built that must ensure today's life saving devices to avoid the risk being hacked.

The problem is when you use your laptop or PC or your Smartphone it's got the number of security features built into firewalls maybe antivirus, address space randomizations but these requirements seem to be missing from the internet of things. Don't buy IoT product if we don't sure about its security we can force the hands of the manufacturers to make it safe for us.

If the applications of IoT increase at a rapid rate then it is difficult to handle this bulk load of applications in the environment. It also produces the problem of managing and controlling these applications. Failing so, the whole system will be uncomfortable [1]. Due to unavailability of special methods, security is les on server side. Any intruder or attacker can attack victims and can break the whole home system. There may be a problem of connectivity [4]. So, achieving connectivity is a challenge at any place and at any time [4].

References

[1] Ming Wang, Guiqing Zhang, Chenghui Zhang, Jianbin Zhang and Chengdong Li, An IoT-based Appliance Control System for Smart Homes, Fourth International Conference on Intelligent Control and Information Processing (ICICIP) 9-11 (2013), 744-747.

[2] J. King, A. A.-Informatica and undefined, A distributed security mechanism for resource-constrained IoT devices, Informatica.si. 2016.

[3] O. Vermesan and P. Friess, Internet of things: converging technologies for smart environments and integrated ecosystems. 2013.

[4] Sarita Agrawal and Manik Lal Das, Internet of Things-A Paradigm Shift of Future Internet Applications, International Conference on Current Trends in Technology, December, 2011.

[5] G. Mantas, D. Lymberopoulos and N. Komninos, Security in Smart Home Environment, 2011.

[6] S. Lee, J. Kim and T. Shon, User privacy-enhanced security architecture for home area network of Smartgrid, Multimed. Tools Appl.

[7] A. Jose, R. M.-Smart CR and undefined 2015, Smart home automation security, researchgate.net.

[8] G. Agosta, A. Antonini, A. B.-S. T. and undefined 2015, Cyber-security analysis and evaluation for smart home management solutions, ieeexplore.ieee.org.

[9] S. Chitnis, N. Deshpande and A. Shaligram, An Investigative Study for Smart Home Security: Issues, Challenges, and Countermeasures, Wirel. Sens. Netw. 08(04) (2016), 61-68.

[10] C. Huth, J. Zibuschka, P. Duplys and T. Guneysu, Securing systems on the Internet of Things via physical properties of devices and communications, in 2015 Annual IEEE Systems Conference (SysCon) Proceedings, 2015, pp. 8-13.

[11] J. Greensmith and Julie, Securing the Internet of Things with Responsive Artificial Immune Systems, in Proceedings of 2015 on Genetic and Evolutionary Computation Conference-GECCO 15, 2015, pp. 113-120.

[12] R. A. Rahman and B. Shah, Security analysis of IoT protocols: A focus in CoAP, in 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), 2016, pp. 1-7.

[13] V. L. Shivraj, M. A. Rajan, M. Singh and P. Balamuralidhar, One time password authentication scheme based on elliptic curves for Internet of Things (IoT), in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015, pp.

[14] A. O. Santin, J. E. Marynowski, A. Witkovski, A. Santin, V. Abreu and J. Marynowski, An IdM and Key-based Authentication Method for providing Single Sign-On in IoT Secure E-Voting System View project Testing the Fault Tolerance and Security of Map Reduce Systems View project An IdM and Key-based Authentication Method for providing Single Sign-On in IoT.

[15] P. Rajiv, R. Raj and M. Chandra, Email based remote access and surveillance system for smart home infrastructure, Perspect. Sci., vol. 8 (2016), 459-461.

[16] A. Ukil, S. Bandyopadhyay and A. Pal, Privacy for IoT: Involuntary privacy enablement for smart energy systems, in 2015 IEEE International Conference on Communications (ICC), 2015, pp. 536-541.

[17] D. Konidala, D. Kim, C. Y.-J. of I. and undefined 2011, Security framework for RFID-based applications in smart home environment, koreascience.or.kr.

[18] O. Tomanek and L. Kencl, Security and privacy of using AllJoyn IoT framework at home and beyond, in 2016 2nd International Conference on Intelligent Green Building and Smart Grid (IGBSG), 2016, pp. 1-6.

[19] T. Mantoro, M. A. Ayu and S. M. binti Mahmod, Securing the authentication and message integrity for Smart Home using smart phone, in 2014 International Conference on Multimedia Computing and Systems (ICMCS), 2014, pp. 985-989.