Privacy and Security issues in IoT based Smart Home Applications

H Manoj T Gadiyar[1], Dr. Thyagaraju G S[2], Bhavya T P[3], Bhavana[3], Mamatha[3], Ahana R[3]
[1]Assistant Professor,Department of CSE,SDMIT,Ujire
[2]Professor,Department of CSE,SDMIT,Ujire
[3]Students,Department of CSE,SDMIT,Ujire

***Abstract*—Internet of Things (IoT) can support numerous applications and services in various domains, such as smart cities and smart homes. IoT smart objects interact with other components e.g., proxies, mobile devices, and data collectors, for management, data sharing and other activities in the context of the provided service. Sensors integrated at different places in homes, offices, and even in clothes, equipment, and utilities are used to sense and monitor owners' positions, movements, required signs, valuable usage, temperature and humidity levels of rooms, etc. Along with sensing and monitoring capabilities, sensors cooperate and communicate with themselves to deliver; share and process sensed information and help real-time decision making procedures through activate suitable alerts and actions. Often the Internet of Things (IoT) is considered as a single problem domain, with proposed solutions intended to be applied across a wide range of applications. However, the privacy and security needs of critical engineering infrastructure or sensitive commercial operations are very different to the needs of a domestic Smart Home environment. Due to internet-connected, dynamic and heterogeneous nature of smart home environment creates new security, authentication and privacy challenges.In this paper, we investigate security attacks in smart home and evaluate their impact on the overall system security. We identified security requirements and solutions in the smart home environment. Also, we have tried to provide solutions for few authentication issues.**

***Index Terms*—Enter key words or phrases in alphabetical order, separated by commas. For a list of suggested keywords, send a blank e-mail to** keywords@ieee.org **or visit** http://www.ieee.org/organizations/pubs/ani_prod/keywrd98.txt

I. INTRODUCTION

The Internet of Things (IoT) has gained traction in recent years as a term to describe the connection of non-traditional devices, such as factory machinery, medical equipment or domestic appliances, to the Internet. Over the past few decades, the use of microprocessor-based controllers in applications from toasters to airliners has become ubiquitous. IoT can be seen as the next step in the evolution of these controllers by connecting them to the Internet. The development of new type of sensors and actuators combined with the deployment of increasingly powerful and pervasive network connectivity's is shaping the concept of the Internet of Things (IoT). Several factors are contributing to the evolution of the current Internet into IoT including the lower market price of IoT devices and the higher demand of customers for new services. In our project, we first identified the security and privacy challenges in iot smart home challenges. In this paper, we identified few major security challenges in IoT and have tried to find the solution for few of these problems using a log-in authentication system and an encryption mechanism.

II. IOT BASED SMART HOME ARCHITECTURE

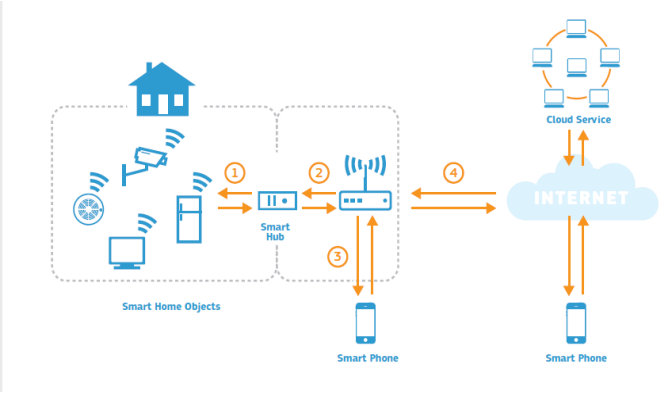

Fig. 1. Architecture of a Smart Home

II. BACKGROUND AND PRIOR WORK

The paper[1] is on a Smart Home scenario. In this scenario, the potential for privacy breaches is limited. However, the activities of these individuals can be indirectly tracked through physical activities of their connected domestic devices, assisted living systems, or smart meters. The protection of privacy in these complex scenarios where different entities and IoT technologies coexist and work together requires new approaches and solutions. They have set up the scene for a security and privacy threat analysis for a typical smart home architecture that relies on existing and readily available market IoT devices and platforms. In contrast to existing security and threat analysis of IoT scenarios, they targeted a real IoT smart home environment deployed in our testbed focusing on the interactions among the different IoT components. In their architecture, they identified points of interest that an adversary might manipulate either to gain access to unauthorized information or to cause a denial of service. Their contribution, in addition to a concrete threat analysis, is a practical feasibility evaluation of the identified vulnerabilities showing how exploits can be implemented in practice. One major issue in their paper is the possibility to deploy IoT installations using the default configurations. They recommended to force users

to properly configure the devices, otherwise the services cannot be started.

Lin[8] explains key future requirements for trusted Smart Home systems. A gateway architecture is selected as the most appropriate for resource-constrained devices, and for high system availability. Two key technologies to assist system auto-management are identified. Firstly, support for system auto-configuration will enhance system security. Secondly, the automatic update of system software and firmware is needed to maintain on going secure system operation. Additionally, RFID (radio frequency identification) tags are seen as an IoT technology for making the location and, potentially, the status of tagged objects available on the Internet. He have explained the range of different application areas in which IoT technology is having an impact will be explored to show that IoT is not a "one-size-fits-all" technology set, and particular emphasis will be placed on IoT as applied to Smart Home applications. Later describes security threats and vulnerabilities in the Smart Home. He have prepared architecture supported by web-services for automatic device and network configuration and automatic system updates is our preferred approach for solving these problems. This paper presents particular challenges to security and privacy. The two main contributions of his paper are to summarize existing network techniques that can be used to secure Smart Homes, and then to present two areas of particular concern(system auto-configuration and security updates) where further work is needed.

In paper[3], authors investigated security issues in the smart home environment using several scenarios. They investigated the security threats, classified these threats according to security objectives and evaluated their impact on the overall system. They identified security requirements and their solutions in the smart home environment. Based on several scenarios, they have set security goals for the smart home. Based on historical data, forecasted of security attacks (like malware, virus, etc.) that how many attacks are expected to be launched in coming five years. They describe open issues and future direction for researchers.

III. SECURITY CHALLENGES IN SMART HOME ENVIRONMENT

In smart home, adversaries can eavesdrop the underlying communication and extract different information due to the lack of an end-to-end encryption between the different components of IoT. It is also a flaw for the existing protocols that IoT builds on; for instance, the SSDP protocol does not use any encryption and thus the adversary could exploit this fact and identify available smart hubs and their capabilities.

Protection against DoS and their distributed counterpart (DDoS) is a challenging task especially for IoT architecture Considering limited capabilities, while currently we even lack effective solutions for IP based services that are supported by high power security infrastructures. The majority of low cost IoT manufacturers do not usually consider mechanisms for validating firm ware integrity during installations, upgrades and on execution, for instance using a trusted boot, IoT devices are exposed to possible software flaws.

One major issue is the possibility to deploy IoT installations using the default configurations.

1. Compatibility: Currently, there is no international standard of compatibility for the tagging and monitoring equipment. They believe this disadvantage is the most easy to overcome. The manufacturing companies of this equipment just need to agree to a standard, such as Bluetooth, USB, etc.
2. Complexity: As with all complex systems, there are more opportunities of failure. With the Internet of Things, failures could sky rocket. For instance, let's say that both you and your spouse each get a message saying that your milk has expired, and both of you stop at a store on your way home, and you both purchase milk. As a result, you and your spouse have purchased twice the amount that you both need. Or maybe a bug in the software ends up automatically ordering a new ink cartridge for your printer each and every hour for a few days, or at least after each power failure, when you only need a single replacement.
3. Privacy/Security: With all of this IoT data being transmitted, the risk of losing privacy increases. For instance, how well encrypted will the data be kept and transmitted with? Do you want your neighbors or employers to know what medications that you are taking or your financial situation?
4. Safety: Imagine if a notorious hacker changes your prescription. Or if a store automatically ships you an equivalent product that you are allergic to, or a flavor that you do not like, or a product that is already expired. As a result, safety is ultimately in the hands of the consumer to verify any and all automation.

The wireless nature of the communication between sensors and devices makes these objectives more vulnerable, as there is no apparent physical boundary of the transmission medium WSNs can suffer from the Denial of Service(DoS) attacks [11] which occur when attackers use PC or laptops to transmit signals in order to interfere with the radio frequencies being used by the network. This kind of DoS can also be visible at the data link layer where, in order to disrupt the communication protocols whether they are industry standards such as IEEE 802.15.4 or ZigBee, attacks are committed by transmitting a continuous stream of messages with a view to generating collisions. These collisions lead sensors to retransmit messages indefinitely and render them inoperative by exhausting battery power. As a result, the sensors consume their valuable computational resources, such as bandwidth and processor time. Other problems include disruption of configuration information, such as routing information, and obstruction of the communication media between the intended users so that they can no longer communicate adequately. Node compromise is one of the major problems in IOTs that lead to inside attacks. It is a kind of act by which a legitimate node in the network is captured and compromised, that is, reprogrammed by an adversary. A Sinkhole Attack [12] is a type of attack where a malicious node attracts network packets towards it by spreading false routing information to its neighbors in order to make selective forwarding of packets which, in turn, reshapes the network's routing behavior. Type

of attack is the physical attack of the node itself. It deals with the ability of the attacker to gain physical access to sensors.

Trespass:-When the smart door lock would be infected by malicious codes or hacked by security flaws, attacker could trespass on his/her home without destroying a doorway a. This threat could cause the loss of life and property. Monitoring and Personal Information Leakage :-there are many sensors for fire watch, housebreaking, baby monitoring, etc. If these are hacked by malicious codes, attackers could monitor inside the home around the clock

DoS/DDoS :-Attackers access smart home network illegally and send messages such as RTS(Request to Send)/CTS(Clear to Send) to smart devices in bulk. They also infect a target device using malicious codes and perform dos attack to a target device or other devices in smart home network.

Falsification :-When smart devices communicate application server, attacker could gather packets by manipulating routing table in gateway. Even if SSL(Secure Socket Layer) technique is applied, attackers could detour by forged certificate. By doing this, they could falsify the contents or leak confidential information.

IV. CONCLUSION

IoT architectures will be an important component of future Internet as it closes the gap between physical and virtual objects. Among others, smart home is one of the main developments of IoT environments as it enhances the user's experience when using home devices.

Albeit the advantages that IoT offers to smart home users do not only expose homes to well known attacks but also the (IoT) sensors should deal with flaws that have not been previously considered. This is due to the fact that such devices are of limited processing power, and rely on heterogeneous network architectures that increase the attack surface of the provided service.

In this paper, we made an attempt to provide a survey on the issues of privacy and security of IOTs in smart home environments. We have discussed several security problems and privacy issues that are present in IOTs considering the smart home's conditions including process management, workflow, interference, appliance placement and movement. A number of existing standard solutions have been studied along with their mechanisms to deal with various attacks and threats.

Open issues in the smart home environment are: required a framework for secure communication between internal and external entities, standardized key management is required to ensure confidentiality, tempering or reverse in smart meter and legal and strong framework for privacy of user. In future of smart home, this problem could become a common case.In this paper, we detect the security threats by making several scenarios and evaluate the impact of these threats on a smart home environment. We studied the recent existing literature of security to identify techniques for prevention against security attacks and using these techniques, we set security goals for the smart home. In future, we proposed a strong framework for user authentication in the smart home.

V. REFERENCES

[1] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino Gary Steri, and Gianmarco Baldini "Security and Privacy Issues for an IoT based Smart Home" MIPRO 2017, May 22- 26, 2017, Opatija, Croatia.

[2] Drushti Desai1, Hardik Upadhyay2 "Security and Privacy Consideration for Internet of Things in Smart Home Environments " Volume 10, Issue 11 (November 2014), PP.73-83.

[3] Eric Zeng, Shrirang Mare, Franziska Roesner "End User Security & Privacy Concerns with Smart Homes".

[4] Waqar Ali, Ghulam Dustgeer, Muhammad Awais, Munam Ali Shah "IoT based Smart Home: Security Challenges, Security Requirements and Solutions ".

[5] Ali Dorri∗, Salil S. Kanhere ∗, Raja Jurdak† and Praveen Gauravaram "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home".

[6] Arunan Sivanathan∗, Daniel Sherratt∗, Hassan Habibi Gharakheili∗, Vijay Sivaraman∗ and Arun Vishwanath "Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices".

[7] Seokung Yoon1, Haeryong Park1, and Hyeong Seon Yoo2 "Security Issues on Smarthome in IoT Environment ".

[8] Huichen Lin and Neil W. Bergmann "IoT Privacy and Security Challenges for Smart Home Environments".

[9] Liane Margarida Rockenbach Tarouco, Leandro Márcio Bertholdo, Lisandro Zambenedetti Granville, Lucas Mendes Ribeiro Arbiza, Felipe Carbone, Marcelo Marotta, José Jair Cardoso de Santanna "Internet of Things in Healthcare : Interoperatibility and Security Issues ".