Research Report – Digital Literacy

Name : Haris Ar-Rasyid
NIK : 023201905032
Study : MM Tech 2019, 2nd batch
President University

ABSTRACT

Security and Privacy Concern over IoT Based Smart Home Environment

Security issues are often second or even last in the list of things that are considered important in a system, however, the information within the system that fall into the possession of certain parties (such as business opponents) can trigger damage to the information owner (Rahardjo, 1998-2005). Smart home is an IoT environment in which various IoT-based or smart home-installed devices are linked to the IoT network such that they can be turned on and off via mobile, at certain hours or while certain activities take place (Bobby & Usha, 2018). The number of malware and malicious entities that aim to hack these IoT systems is increasing as the IoT model extends to sensitive people like government officials and business owners (Mangino, Pour, & Bou-Harb, 2020). Although the essence of smart home protection danger is identical to other IoT-based settings, which are anonymity, authentication and entry, the greatest weakness is the shortage of qualified protection specialists capable of handling the complexity of a smart home network (Lin & Bergmann, 2016). The availability of information and communication resources is a major security challenge and can often be hindered by attacks (Cvitić, Perakovic, Periša, & Botica, 2018). A specific concern is that network protection is primarily based on the deployment and setup by untrained staff. The best solution for addressing protection and privacy problems is a smart home gateway architecture assisted by web-services for automatic device and network configuration and automatic software updates.

Keywords: *Security, Privacy, IoT, Smart Home Environment, Network.*

I. INTRODUCTION

The extension of the IoT model is particularly evident on the consumer market, as companies and smart homes adopt such emerging technologies, as more than 70 per cent of all North American households have at least one IoT system connected to the Internet, and the global average of 40 per cent indicates an upward trend (Mangino, Pour, & Bou-Harb, 2020). Our conventional devices and appliances are going to be smarter, our lifestyle can be changed with modern technology, smart home technology and IoT will give people the insight they need to live better lives — longer, healthier and happier (Bobby & Usha, 2018). Although organizations may commit specialized specialist expertise to network protection and device layout design, the smart home is mostly a fairly ad hoc program without dedicated system management services and without the householder's in-depth technological knowledge (Lin & Bergmann, 2016).

Unprotected computers are at risk of being infected when malicious organizations endanger the reliability, safety and protection of their operating environments, and may have a direct impact on the system owner (Mangino, Pour, & Bou-Harb, 2020). Numerous studies have identified the security challenges associated with unauthorized data modification in a smart home environment, inserting malicious code (Cvitić, Perakovic, Periša, & Botica, 2018). Smart home design would ensure the suitability and secrecy of the transmitted data as a major necessity to maintain robustness and efficiency at the service level and to promote protection (Bobby & Usha, 2018). Intelligent home ecosystem with improved anonymity, data security strategies and ethical standards can certainly earn consumer respect and achieve strategic edge in the connected world (Mohammed & Qayyum, 2017).

The prediction for the number of IoT devices will reach approximately 20 to 50 billion in 2020 where the majority of the usage belongs to the individual consumers (Badirova, 2018). Millions of devices interconnected with all of this IoT data being transmitted, the risk of losing privacy increases and concerns over privacy increased more than ever (Bobby & Usha, 2018). With that said, the IoT will impact such large effects on society in multiple ways, it is imperative that IoT-based systems should exhibit some level of secure, reliable, and private behaviors, as well as other attributes generally associated with quality (Bojanova & Voas, 2017). This research will identify the requirement, threats/challenges, and countermeasures in term of security and privacy concern. The results of the research should provide at least a basis for further research for the development of IoT based smart home environment.

II. LITERATURE REVIEW

II.1. The Internet of Things

The Internet of Things (IoT) is generally defined as any device that can connect to the Internet, interact with other devices and exchange data. (Mangino, Pour, & Bou-Harb, 2020). In recent years, IoT has gained traction as a term for describing the connection to the Internet of non-traditional devices, such as factory machinery, medical equipment or domestic appliances (Lin & Bergmann, 2016). In a more technical definition, IoT is an advanced automation and analytical system that exploits networking, sensing, big data and artificial intelligence technology to deliver complete systems that enable greater transparency, control and performance when applied to any industry or system (Bobby & Usha, 2018).

Characteristic for the IoT concept can be observed via a layered architecture consisting of four basic layers (perception, network, middleware and application) as seen in Figure 1 (Cvitić, Perakovic, Periša, & Botica, 2018). Traditionally, the components needed for IoT are the sensors for collecting the information, the Wi-Fi passes this information to a server and the control panel reacts when the data flag issues are resolved automatically or the problems can be resolved manually (Bobby & Usha, 2018). As most IoT devices use a low-end microcontroller and the current Internet protocols are not usually built for such embedded devices, standardization of the IETF (Internet Engineering Task Force) has played a vital role in defining the required lightweight connectivity protocols for restricted environments over the established IP network (Lin & Bergmann, 2016).

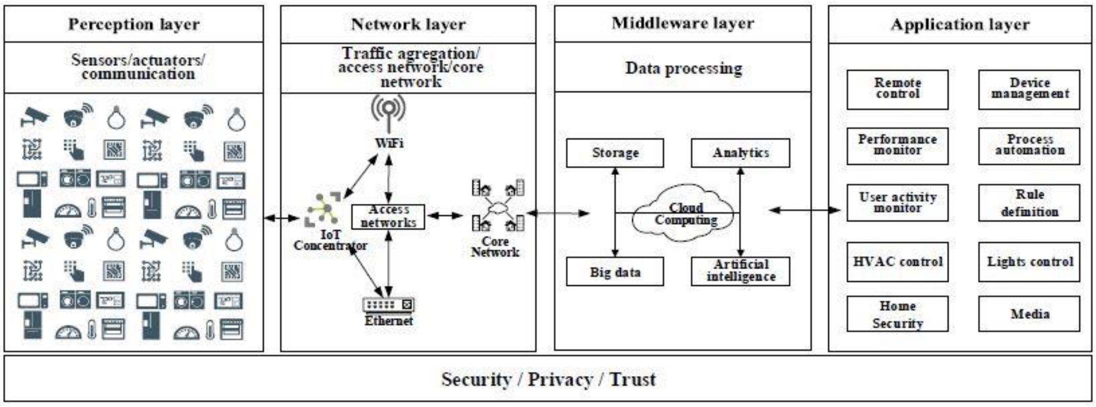

Figure 1. Architecture of IoT (Cvitić, Perakovic, Periša, & Botica, 2018)

II.2. Smart Home Environment

Smart home is an IoT environment in which various IoT-based or intelligent home-installed appliances are linked to the IoT network so that they can be turned on and off by certain users at certain hours or while certain activities take place (Bobby & Usha, 2018). Smart Home provides improved convenience and protection as well as enhanced ecological resilience, such as a smart air conditioning device that can monitor position data to achieve the optimal degree of comfort when the house is occupied and conserve electricity when it is not occupied (Lin & Bergmann, 2016). Smart home systems may be grouped into three common groups: home surveillance/control tracking, electrical home appliances and home multimedia as shown in Figure 2 (Cvitić, Perakovic, Periša, & Botica, 2018).

There are three broadly categorized components of an IoT automated house that are vital to building a smart home: hardware, software, and communication protocol (Bobby & Usha, 2018). Short range technologies such as IEEE 802.15.4 ZigBee, ITU-T G.9959 Z-Wave, or Bluetooth Low Energy are the most frequently used (Cvitić, Perakovic, Periša, & Botica, 2018). Along with the communication protocol, another crucial component of the IoT network is the firmware (Bobby & Usha, 2018). The majority of smart-home service belongs to personal home assistants like Amazon Alexa, Google Home, smart security systems, home-related smart meters and so on (Badirova, 2018). Middleware, web, and gateway architectures are among the three most significant and common smart home architectures (Lin & Bergmann, 2016).

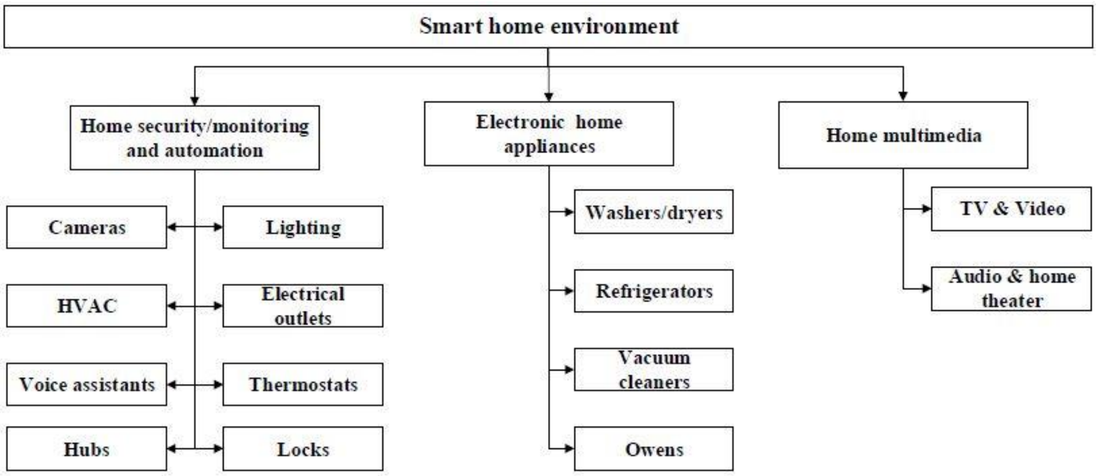

Figure 2. Smart Home Devices (Cvitić, Perakovic, Periša, & Botica, 2018)

II.3. Information System Security

Majority of researchers and experts have confirmed that securing the IoT system is one of the most serious challenges that stand in the way of successful adoption of IoT devices (Atlam & Wills, 2020). Computer security covers six aspects, namely confidentiality, integrity, authentication, availability, access control, and non-repudiation (Rahardjo, 1998-2005). In particular, cybersecurity covers three main themes: confidentiality, authentication and access (Lin & Bergmann, 2016). Security threats were defined by the extent of what acts an intruder may take after a system has been effectively compromised, and the volume of data that may be taken or destroyed (Mangino, Pour, & Bou-Harb, 2020). A framework is planned, agreed and recognized to be called safety-critical, supervisory and governance (Bojanova & Voas, 2017).

Attacks on information system security can be seen from the point of view of the role of a computer or computer network whose function is as a provider of information (Rahardjo, 1998-2005). The interconnected nature of the Internet means that web resources can be attacked from anywhere in the world, making cybersecurity a key issue (Lin & Bergmann, 2016). The IoT is a dynamic system in which every poorly secured object can disturb the security of the entire system as they connected (Atlam & Wills, 2020). Security operations will constantly enforce new policies to effectively mitigate the regularly changing ransomware, phishing scams and related attacks on a network and its infrastructure (Mangino, Pour, & Bou-Harb, 2020).

II.4. Information/Data Privacy

The main core aspect of privacy or confidentiality is an effort to safeguard data/information that is private, or provided only to certain parties for certain purposes, from people who are not entitled to access (Rahardjo, 1998-2005). Technology and thus IoT are continuously evolving and reviewing systems which have both benefits and threats, and often individual users/consumers are at risk (Badirova, 2018). Privacy is a notion associated with four main elements: information relating to different types of personal data, communication between two communicating nodes, physical safety alongside any external damage, and territorial limits or physical space concerned (Atlam & Wills, 2020). Several privacy threats related to information / data are mainly aimed at obtaining the right to recognize the user, the position of the personal data and the profiling (Badirova, 2018).

III. ANALYSIS AND DISCUSSION

III.1. Smart Home Security/Privacy Requirement

Computer security covers six aspects, namely confidentiality, integrity, authentication, availability, access control, and non-repudiation (Rahardjo, 1998-2005). The privacy problems in relation to smart home revolve around confidentiality, authentication and access management (Alhalafi & Veeraraghavan, 2019). In addition, the smart home system should employ typical CIA (confidentiality, integrity and availability) security requirements (Atlam & Wills, 2020). Privacy within the smart home can be classified into three categories: awareness of the risks to privacy imposed, individual control over the collection and processing of personal information, and awareness of the subsequent use and dissemination of personal information outside personal control (Shaikh, Mohiuddin, & Manzoor, 2019).

Confidentiality refers to the need to ensure that data are kept private with only the users authorized to access the data (Alhalafi & Veeraraghavan, 2019). Integrity is used to guarantee the content of messages exchanged are protected against manipulation by an intruder without being able to track this manipulation (Atlam & Wills, 2020). The authentication process ensures the data received is original and can be trusted (Mohammed & Qayyum, 2017). Availability is used to insure that a malicious individual can not intervene or damage the contact or standard of service delivered by devices or the network (Atlam & Wills, 2020). Access control ensures only authorized users can retrieve information while ensuring that the authorized users are not prevented from obtaining the data (Alhalafi & Veeraraghavan, 2019).

Although these things are important for the smart home, there are certain safety criteria that need to be enforced for each stage of the smart home architecture as shown in Figure 3 (Atlam & Wills, 2020). Node authentication is the main requirement for the physical layer, lightweight cryptographic algorithm encrypt transmitted data, and identity authentication for the connectivity/network layer (Cvitić, Perakovic, Periša, & Botica, 2018). For data abstraction, accumulation and edge-computing level, application security are needed to secure data stored in cloud database (Badirova, 2018). While for the application and collaboration level, authentication/key agreement and password management are essential for information security at this level (Mangino, Pour, & Bou-Harb, 2020).

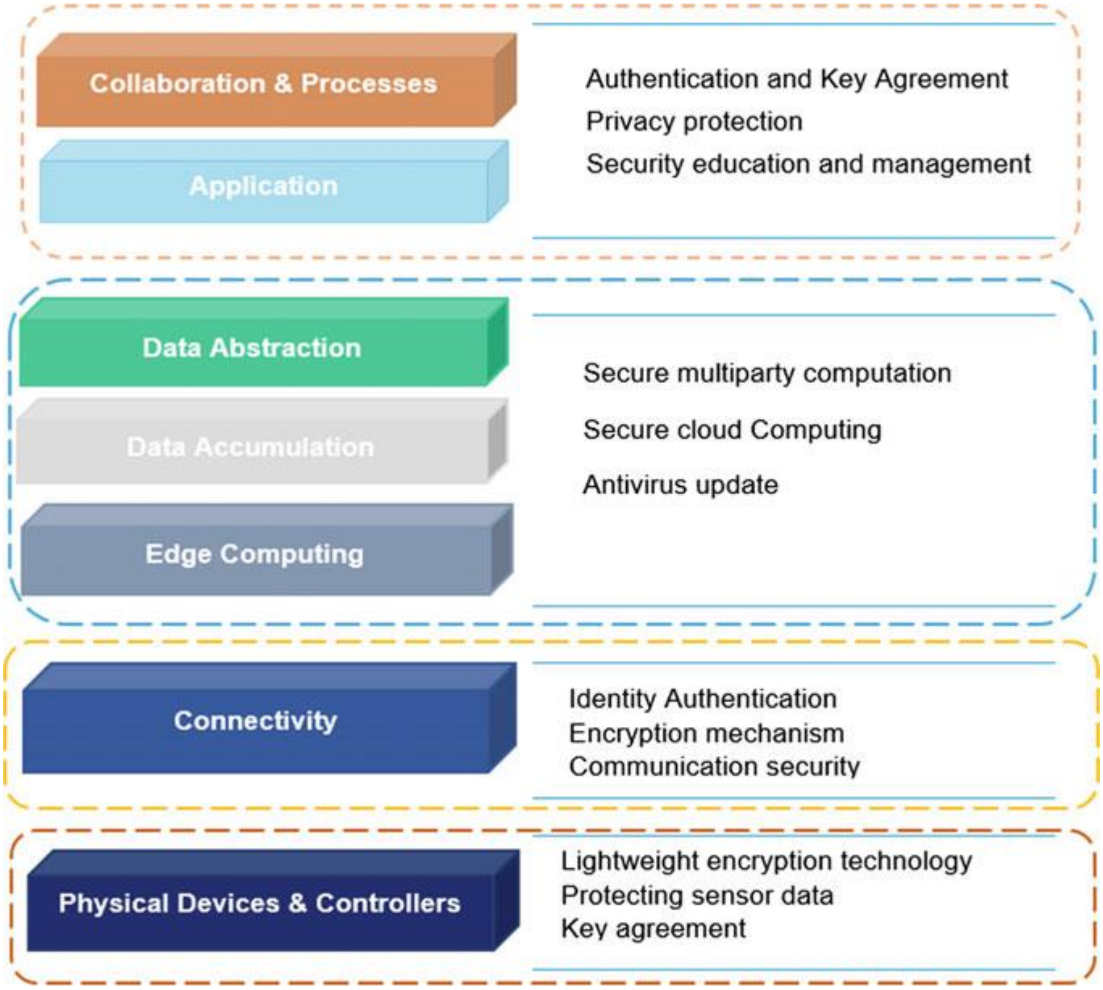

Figure 3. Security Requirements of smart home architecture (Atlam & Wills, 2020).

III.2. Smart Home Security/Privacy Threats & Challenges

Important weaknesses in the smart home setting include device usability, physical connectivity, limited machine infrastructure, complexity of the framework, set software, poor adoption of standards and the scarcity of qualified technology specialists who can handle the complexities of a smart home network (Lin & Bergmann, 2016). Identification, localization, monitoring, authentication, lifecycle changes and product attacks are many issues facing individuals inside smart home environments (Alhalafi & Veeraraghavan, 2019). The distributed and dynamic smart home system creates weak communication channels that malicious objects use to exploit and open up new threats to track, monitor and report actions of users (Atlam & Wills, 2020). One of the main reasons why smart home devices are more appealing to attackers is that they work primarily on public clouds, making it easy to reach them even without accessing the system itself (Badirova, 2018).

The smart home system contains four major types of attacks, physical, software, network, and encryption attacks as seen in Figure 4 (Atlam & Wills, 2020). It's hard to avoid unauthorized physical access as all smart home systems have a physical sensor and its data can be modified (Mohammed & Qayyum, 2017). Software attacks are the key of most security breaches by utilizing contact interfaces to exploit vulnerabilities contained in program implementation (Atlam & Wills, 2020). In network attacks, attacker takes over a node within network and pulls all traffic from adjacent nodes using the routing algorithm to selectively forward, alter, or erase packets (Mohammed & Qayyum, 2017). Encryption attacks depend on breaking the mechanism of security used in the smart home system (Atlam & Wills, 2020).

Physical Attacks

Node Tampering : This attack targets the sensor node by physically damaging it or even replaces the entire node or part of its hardware to gain the access.

RF Interference on RFIDs : The attacker uses RFID tag to direct noise signals using the Radio Frequency signals used by RFIDs. These signals affect the quality of communication.

Malicious Node Injection : The attacker physically operating a new malicious node between nodes within smart home system, which allows the attacker to control data flow between nodes.

Malicious Code Injection : This attack focuses on physically injecting the node with malicious code to gain access to the smart home system.

Physical Damage : This type of attack requires the attacker to reach area or building to destroy it. The attacker harm the smart home system directly to affect system availability and quality.

Sleep Deprivation : The sleep deprivation attack retains the nodes running at all times which leads to more energy feasting that results in shutting down of nodes after consuming battery.

Social Engineering : The attacker uses the lack of security awareness of users to manipulate and gain access to the smart home system to collect sensitive information or to accomplish particular activities to serve his goals.

Software Attacks

Malicious Scripts : Since the smart home system is linked to the Internet, the attacker uses this facility to create malicious scripts that aim to gain access to disturb system availability.

Phishing Attacks : It is a kind of social engineering attack which targets user login credentials and other sensitive information through infected emails or phishing websites.

Virus/Worms/Spyware : This type of attack is closed to malicious code injection attack in which the attacker injects the system with malicious software to gain access to the system.

DoS Attack : An attacker can perform Denial of Service (DoS) on the smart home system across the application layer which affects all users of the smart home network. This type of attack blocks legal users and gives the attacker full access to sensitive data.

Network Attacks

Traffic Analysis Attacks : This attack is concerned with sniffing out sensitive data due to their wireless features. It is necessary to collect some network information before operating any attacks by using a traffic analysis attack.

RFID Spoofing : This type of attack obtain data stored on an RFID tag using the original tag ID to send its own data to appear to be from the original source as a legal node.

RFID Cloning : This type of attack targets RFID tag by copying its own data to another RFID tag although it does not duplicate the original ID of the RFID.

Unauthorized Access : Due to the lack of appropriate authentication techniques in most nodes, it is easy to be hacked by anyone allowing the intruder to read, edit or even delete data on nodes according to his goals.

Sinkhole Attack : This type of attack targets the confidentiality of data and disrupt network service by discarding all packets instead of forwarding them to the desired destination.

MITM Attack : Man-In-The-Middle (MITM) attack place a malicious node between two communicating nodes to intercept and monitor all traffic sent between them.

Routing Info Attacks : Routing table information is used by the network router to forward data to their desired destinations. This attack spoof or change its contents to disrupt network service and error messages will be sent.

Encryption Attacks

Side Channel Attacks : This attack targets encryption devices in the smart home system using certain techniques to reach encryption and decryption keys used in the data encryption process.

Cryptanalysis Attacks : If the attacker already has cipher-text or plaintext, then the attacker’s goal becomes to find the encryption key by breaking the system encryption structure using cryptanalysis attacks.

MITM Attack : Two nodes communicate using an encryption algorithm, they exchange encryption and decryption key. MITM intercepts signals sent between two nodes and tries to execute a key exchange with each node separately.

The privacy issues of the smart home network contribute to the possibility of associating an object such as an address with the user and relevant data (Alhalafi & Veeraraghavan, 2019). The main challenge is to connect the identification with a specific context which violates the privacy of the individual by providing the identifying information to individuals outside the personal sphere of the user (Atlam & Wills, 2020). Another challenge to privacy is the ability to identify and monitor the individual's position through space and time, because many users may view it as a violation of privacy if the data is misused or if they have little discretion about the sharing of their location data (Alhalafi & Veeraraghavan, 2019).

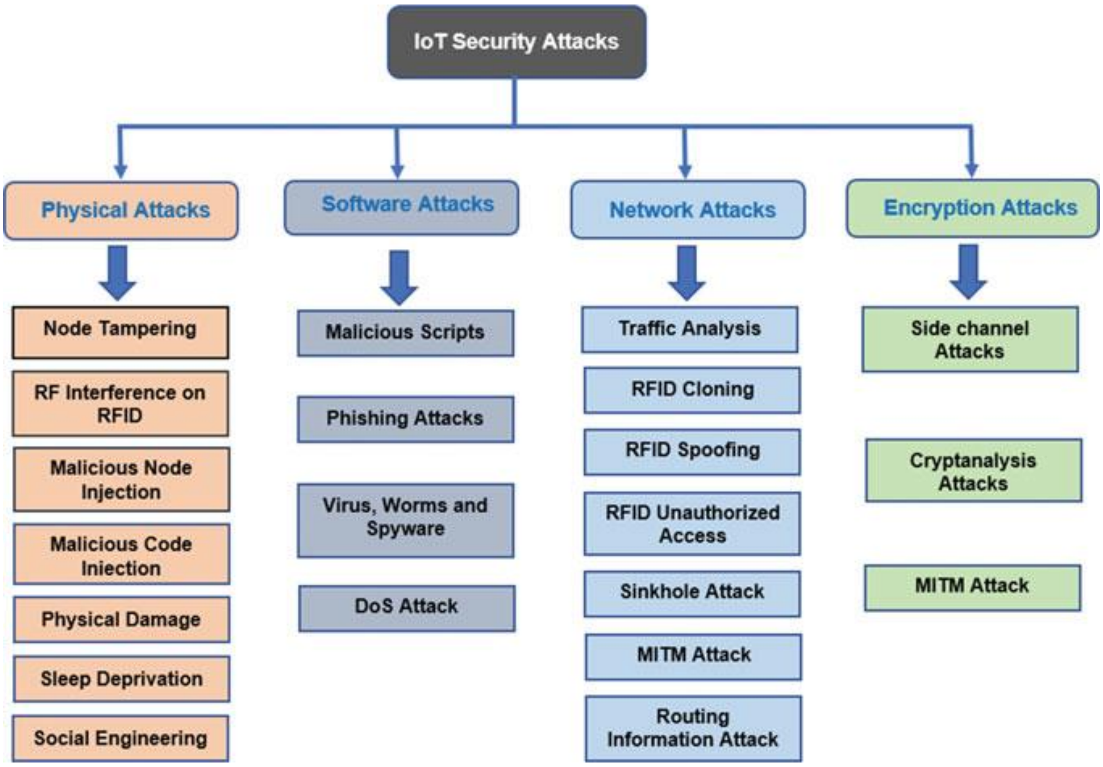

Figure 4. Various attacks in the smart home (IoT) system (Atlam & Wills, 2020).

III.3. Smart Home Security/Privacy Countermeasures

General approaches for keeping the smart home environment more safe include installing protection software on the computer, enforcing roll-based access control scheme, introducing app/endpoint authentication, filtering packets, and avoiding malicious firewalls and intrusion prevention systems (Badirova, 2018). In order to achieve secure communication, the smart home environment must include services such as encryption, end-to-end environments and real-time and critical infrastructure protection access control (Mohammed & Qayyum, 2017). In order to protect the privacy of the smart home community, systems should use suitable cryptographic techniques to restrict who can access it, and smart home service providers can use data minimization by limiting the processing of personal data to just what applies to the service they offer (Atlam & Wills, 2020).

In particular, security and privacy solutions for Wireless Sensor Networks (WSN) type smart home devices are shared keys, protected grouping, encryption and secure data aggregation, while RFID type devices are physical methods such as kill tag, faraday net or stop tag, and security protocols such as two-way authentication protocol (Shaikh, Mohiuddin, & Manzoor, 2019). In terms of smart home architecture, gateway architecture is preferable since it can implement sophisticated firewall and proxy support for IoT devices even in the temporary absence of an internet connection so that they are minimally exposed to direct network attacks, and it can also work with resource-constrained IoT devices without complex middleware (Lin & Bergmann, 2016). One of the key problems of privacy violations is lack of public knowledge and thus smart home consumers need to be well conscious of how to remain safe from some kind of privacy threats (Atlam & Wills, 2020).

A lack of technical support is the biggest challenge in the household smart home environment, thus a secure auto-configuration approach as seen in Figure 5 should be further studied not only to simplify smart home device installation and maintenance but also to enhance the security in the auto-configuration process (Lin & Bergmann, 2016). When a new device is attached to the network, the gateway will use the device ID to interrogate a trusted web-service to discover the details of the device, what its functionality is, what its commands are, what encryption and networking protocols it understands, and any essential firmware updates that are now available (Badirova, 2018). This is a different approach to most auto-configuration approaches which require a lot of this information to be stored on the devices themselves, and for the devices to be able to implement a deep protocol stack (Lin & Bergmann, 2016).

There are many methods proposed for safeguarding privacy (Atlam & Wills, 2020). Smart home consumers will have the requisite flexibility to monitor their own information and to decide who can access it. Built-in mechanisms for protecting the privacy of consumers must be designed as an integral part of every device (Bojanova & Voas, 2017). Smart home consumers need to be well informed of how to defend themselves from some form of threat to privacy. The principle of data minimization will be followed by smart home service providers by growing the processing of personal data to just what is relevant to the service they offer. Smart home devices will use suitable cryptographic technique to encrypt the data. One of the strategies to safeguard the privacy of smart home users is to include an effective access control model for the smart home network to allow smart devices to make fine-grained decisions (Shaikh, Mohiuddin, & Manzoor, 2019).

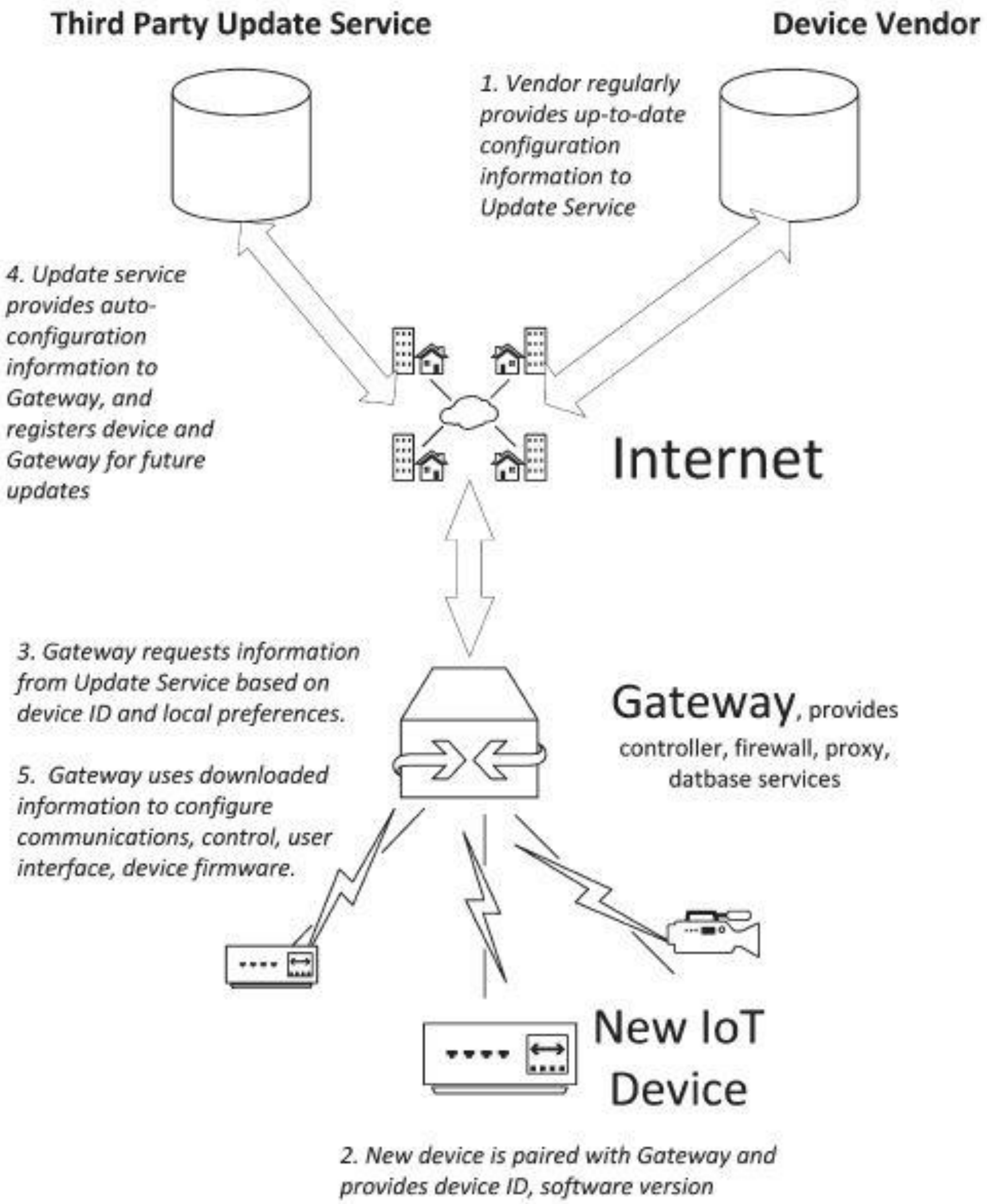
Third Party Update Service
Device Vendor
1. Vendor regularly provides up-to-date configuration information to Update Service
4. Update service provides auto-configuration information to Gateway, and registers device and Gateway for future updates
Internet
3. Gateway requests information from Update Service based on device ID and local preferences.
5. Gateway uses downloaded information to configure communications, control, user interface, device firmware.
Gateway, provides controller, firewall, proxy, datbase services
New IoT Device
2. New device is paired with Gateway and provides device ID, software version

Figure 5. Auto-configuration in smart home architecture (Lin & Bergmann, 2016).

IV. CONCLUSION & RECOMMENDATION

Security is a big problem on smart home environment that needs to be solved in order to embrace and utilize the networks in different areas of human activity such as commerce and entertainment. Device level security and safety, consumer authentication and encryption of communication links are important for smart home safe operations. Privacy standards require that consumers will be allowed to hold their details under surveillance, as well as being able to opt out of the smart world without any adverse repercussions. The Internet of Things is not a common technology area, so the protection strategies utilized in a domestic smart home implementation are very different from those that mission-critical systems of manufacturing or utility would manage. A specific concern is that network protection is primarily based on the deployment and setup by untrained staff. The business industry is especially at risk, since there is no central body controlling the maintenance of electronics and their protection posture.

The best solution for addressing protection and privacy problems is a smart home gateway architecture assisted by web-services for automatic device and network configuration and automatic software updates. Furthermore, smart home system protection plays a significant role in ensuring a stable and secure network and in preventing the smart home device and its components from causing unnecessary danger or physical harm. Further work is needed to build and implement effective protection measures immune to various types of attacks. Users, organizations, and developers therefore need to come under one roof and find a prominent solution for a stable smart home environment. More protection for smart devices & IoT communication's privacy requirements can be anticipated to improve in the future which would enable users to automate activities easily utilizing this technology.

REFERENCES

Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and Security Challenges and Solutions in IOT: A review. *International Conference on Smart Power & Internet Energy Systems* (pp. 1-5). Melbourne, Australia: IOP Publishing, Ltd. Retrieved from https://doi.org/10.1088/1755-1315/322/1/012013

Atlam, H. F., & Wills, G. B. (2020). IoT Security, Privacy, Safety and Ethics. *Digital Twin Technologies and Smart Cities, Internet of Things* (pp. 123-149). Switzerland: Springer Nature. Retrieved from https://doi.org/10.1007/978-3-030-18732-3_8

Badirova, A. (2018). Security and Privacy in Internet of Things. *Applied Computer Science*, 1-8. Retrieved from https://www.researchgate.net/publication/326226121

Bobby, M., & Usha, D. (2018). Privacy Issues In Smart Home Devices Using Internet Of Things – A Survey. *International Journal of Advanced Research, 6*(10), 566-568. Retrieved from https://www.researchgate.net/publication/328761774

Bojanova, I., & Voas, J. (2017). Trusting the Internet of Things. *IT Professional, 19*(5), 15-19. Retrieved from https://www.researchgate.net/publication/320220563

Cvitić, I., Perakovic, D., Periša, M., & Botica, M. (2018). Smart Home IoT Traffic Characteristics as a Basis for DDoS Traffic Detection. *Management of Manufacturing Systems.* Dubrovnik: EAI. Retrieved from https://www.researchgate.net/publication/329410513

Lin, H., & Bergmann, N. W. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Multidisciplinary Digital Publishing Institute - Information, 7*(44), 1-15. Retrieved from https://www.researchgate.net/publication/305311632

Mangino, A., Pour, M. S., & Bou-Harb, E. (2020). Internet-scale Insecurity of Consumer Internet of Things: An Empirical Measurements Perspective. *ACM Transactions on Management Information Systems, 1*(1), 1-25. Retrieved from https://www.researchgate.net/publication/340610825

Mohammed, H., & Qayyum, M. (2017). Internet of Things :A Study on Security and Privacy Threats. *2nd International Conference on Anti-Cyber Crimes (ICACC).* Abha, Saudi Arabia: IEEE. Retrieved from https://www.researchgate.net/publication/316735737

Rahardjo, B. (1998-2005). *Keamanan Sistem Informasi Berbasis Internet.* Bandung: PT Insan Infonesia - Bandung & PT INDOCISC - Jakarta. Retrieved from http://budi.rahardjo.id/files/keamanan.pdf

Shaikh, E., Mohiuddin, I., & Manzoor, A. (2019). Internet of Things (IoT): Security and Privacy Threats. *2nd International Conference on Computer Applications & Information Security.* Riyadh, Saudi Arabia: IEEE. Retrieved from https://www.researchgate.net/publication/334698620