Internet of Things (IoT) of Smart Home: Privacy and Security

Zaied Shouran
Computer and Electronics Science Department, UGM, Yogyakarta

Ahmad Ashari
Computer and Electronics Science Department, UGM, Yogyakarta

Tri Kuntoro Priyambodo
Computer and Electronics Science Department, UGM, Yogyakarta

ABSTRACT
The smart home is an environment, where heterogeneous electronic devices and appliances are networked together to provide smart services in a ubiquitous manner to the individuals. organization and people are wide accepting and adopting the functionalities offered by the smart home applications. this can be because of the various advantages, in easing users' everyday life and work, provided by the rising internet of Things (IoT) technologies and devices, equipped with sensors, cameras, or actuators, and able either to accumulate information from the environment or to perform proper tasks. the main features of smart homes embrace real-time monitoring, remote control, safety from intruders, gas/fire alarm, and so on. Since among smart homes, sensitive and personal data are managed, security and privacy solutions should be put in place, to protect users/businesses' data against violation try still on guarantee the supply of reliable services. As IoT home devices become increasingly ubiquitous, study's findings and recommendations contribute to the broader understanding of users' evolving attitudes towards privacy in smart homes.

Keywords
Internet of Things (IoT), Smart home, Privacy and Security

1. INTRODUCTION
The progress of information and communication technology in the era of globalization is a phenomenon that presents a big challenge for the company to continue to grow and develop. Application of the proper security system and the availability of many security tools that are either pro or anti become a challenge for the emergence of system vulnerability. Also, Network quality and data transmission media can be a factor in the vulnerability of the integrity and availability of information [1]. Various companies continue to adjust, both in terms of products, services, and marketing strategies to be able to compete in their respective markets. in the field of telecommunications services, the company is required to continue to provide the best service in order to maintain the stability of the company as well as get the maximum profit. The use of computers in the future will dominate human work and defeat human computing capabilities such as the use of electronic equipment remotely, using Internet media, IoT (Internet of Things). This allows users to manage and optimize electronic equipment that uses the Internet. This indicates that in the near future computers and electronic equipment are able to exchange information through these means, thereby reducing direct human interaction. This will also increase the number of Internet users with various Internet facilities and services. The main challenge in IoT is to bridge the gap between the physical world and the world of information, such as how to process data obtained from electronic equipment through an interface between users and equipment.

The developing IoT arrange has approached with essential needs for influencing it to secure. A lot of security issues has turned into a challenge for the IoT organize. Security experts have warned of the potential risk of large numbers of unsecured devices connecting to the Internet since the IoT concept was first to propose in the late 1990s. There are Six-Layer IoT Architecture, that is a coding layer, perception layer, network layer, a middleware layer, application layer, and business layer. These all layers also can apply in the Smart Home. The architecture of a common IoT system is divided into three layers: perception layer, network layer, and applications layer. The way in which components are grouped together in the three layers of a generic IoT system is shown in Figure 1.

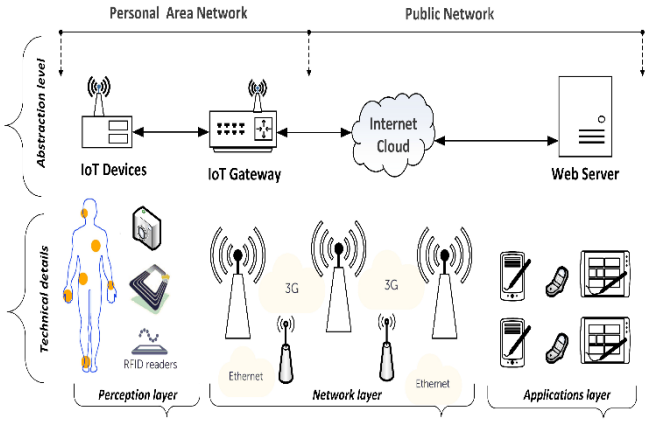

Figure 1. A generic architecture of an IoT system comprises IoT devices, a gateway, and a web server. The figure shows the internal and external sides of the system. The figure was modified from [2].

Security requirements for smart home in a smart home environment, services are provided over the wireless network. An attacker is able to access or invade a smart device on the wireless network. In this study, the security requirements for safe smart home service, including integrity, availability, and authentication.The purpose of the Internet of Things is to allow things to be connected anytime, anywhere, with anything and anyone ideally uses paths or networks and services. The Internet of Things is a new revolution of the Internet. Goods will make themselves easily recognizable and they get intelligence by making or allowing contexts related to the fact that they can communicate information about themselves.This comes together with the emergence of a cloud system or cloud computing that has a transition from the Internet to IPv6 to handle limited capacity [3].

2. LITERATURE REVIEW

Smart home system overview

The IoT smart home services are increasing day by day, digital devices can effectively communicate with each other using Internet Protocol (IP) addresses. All smart home devices are connected to the internet in a smart home environment. As the number of devices increases in the smart home environment, the chances of malicious attacks also increase [4]. If smart home devices are operated independently the chances of malicious attacks also decreases. Presently smart home devices can be accessed through the internet everywhere at any time. So, it increases the chances of malicious attacks on these devices [5].

A smart home consists of four parts: the service platform, smart devices, home gateway, and a home network. In the smart home, many devices are connected and smartly shares information using a home network. Consequently, there exists a home gateway that controls the flow of information among smart devices connected to the external network. Service platform uses the services of a service provider that deliver different services to the home network.

Smart Home Security Objectives

Clearly describing the security goals the smart home environment is expected to meet, serves as the first step in the effort for ensuring unfailing and consistent operation. For the purposes of this paper, consideration six commonly adopted goals described below [6] as the most important for smart home security, these goals are:

Confidentiality: the assurance that data will be disclosed only to authorized individuals or systems.

Integrity: A smart device will be accessed over the wireless network, in order that it needs a security system. an attacker is in a position to insert a malignant software application and alter a service purpose through malicious code. For the reason, while not integrity, the entire smart home system will be infected with malicious code by an attacker and thereby the supply of smart home service can fall. Therefore, the integrity of smart home service is required. to confirm the integrity of smart devices, it is essential to use a hash function and a digital signature for vital data or module codes [7] [8].

Availability: A smart device sends and receives data to and from the surface over a wireless network if it is off-line information, it's capable to fabricate and modify the data. Fictional data can cause malfunction of smart devices that deteriorate a user's convenience of smart devices. deteriorated handiness can lead to service overload, and the malfunction can originate financial losses from a rise in electrical rate and therefore the risk of life. To secure availability, it is necessary to limit different actions from the essential functions and to provide access to functional access [9] [10].

Authenticity: several devices whose security is not taken into consideration. If AN attacker inserts a derived module or a malignant code in an exceedingly smart device, it is potential to contaminate a smart home service environment and make the device used for malicious functions, like distributed denial of service (DDoS), denial of service (DoS), and private data discharge. Moreover, if AN attacker disguises a modified module as a normal module, the module can function the key backdoor for malicious action which may lower the function of the normal module and thereby deteriorate availableness. Therefore, it's needed to provide authentication of a smart device. For the authentication, it is possible to use a certificate [8] [11].

Authorization: the assurance that the access rights of every entity in the system are defined for the purposes of access control[11].

Non-repudiation: the assurance that undeniable proof will exist to verify the truthfulness of any claim of an entity.

There are three different terminologies, secure channel, confidential channel, and authentic channel. A secure channel is a way to do data transfer safely against tampering and overhearing efforts. Meanwhile, the confidential channel is a way to do data transfer that is resistant to overhearing attempts although does not always resist tampering. In addition, the authentic channel is a way to transfer data that is not affected to tampering although not necessarily resistant to overhearing attempts. For the purposes of law enforcement, it is necessary to choose a secure channel because using confidential or authentic channel only is not enough [12].

Security Attacks

Security threats within the smart home environment usually attempt to compromise one or more of the security goals that just described. These threats can be classified into two broad categories. In the first category, namely "passive attacks", this study places attacks attempting to learn or make use of information from the system without affecting system resources. In other words, in passive attacks, the adversary intends to obtain information being transmitted not to modify it but to learn something from it. Passive attacks can take the form of eavesdropping or traffic analysis. By eavesdropping, authors refer to the unauthorized interception of an on-going communication without the consent of the communicating parties. By traffic analysis, authors refer to something subtler. Instead of trying to get hold of message contents, like in an eavesdropping attack, in traffic analysis, the adversary monitors traffic patterns in order to deduce useful information from them. Both of these attacks are considered difficult to detect since they do not alter data. Thus, in dealing with them trying to focus on prevention rather than detection. The second category, namely "active attacks", is the category where place those attacks attempting to alter system resources or affect its operation. Active attacks can involve some modification to data or the introduction of fraudulent data into the system. The most common amongst these attacks are a masquerading, replay, message modification, denial of service and malicious software. A masquerading attack takes place when an intruder pretends to be a legitimate entity to gain privileges. A replay attack involves the passive capture of messages in communication and their retransmission to produce an unauthorized effect. A message modification attack, involves the alteration of the contents of a legitimate message or the delaying or reordering of a stream of messages, aiming to produce an unauthorized effect [11].

A denial of service attack aims to either temporarily or permanently interrupt or suspend the availability of the communication resources of a system. Finally, malicious software attacks, are attacks aiming to exploit internal vulnerabilities to modify, destroy and steal information or gain unauthorized access to system resources [13].

Impact Evaluation

For the assessment of the criticality and sensitivity of certain interactions and the evaluation of the impact level of threats against those interactions within the smart home/smart grid environment, this study adopts FIPS 199, impact level assessment criteria [1]. FIPS199 characterizes potential impact of threats as Low, Moderate or High. Where the potential impact is said to be [13]:

Low (L): if the violation of one or more of the security goals described above can be expected to have a limited adverse effect on smart home operations, assets or individuals. Limited adverse effect could mean the degradation of an entity's capability to efficiently perform its primary functions, minor damage to assets, minor financial losses or minor harm to individuals.

Moderate (M): if the violation of one or more of the security goals described above can be expected to have a significant adverse effect on smart home operations, assets or individuals. Significant adverse effect could mean significant degradation of an entity's capability to efficiently perform its primary functions, significant damage to assets, significant financial losses or significant harm to individuals (not including loss of life or life-threatening injuries).

High (H): if the violation of one or more of the security goals described above can be expected to have a severe or catastrophic adverse effect on smart home operations, assets or individuals. Severe or catastrophic adverse effect could mean severe degradation or loss of an entity's capability to perform its primary functions, major damage to assets, major financial losses or severe harm to individuals.

Table 1 Smart Home Security Issues [13]

Scenario num:	Possible Threads	Security Goals Compromised	Degree of Impact
SH_1	Eavesdropping (N) Traffic Analysis (N) Message Modification (N) Replay Attack (N) EMS Impersonation (SH)	Confidentiality Integrity Authenticity	L-M
SH_2	Repudiation (N) Message Modification(N) Replay Attack (N)	Non repudiation Integrity Authentication	M
SH_3	Tampering/Reversal/ Removal of Meter (SH) Illegal Software Modification/Update(SH)	Authentication Integrity	L
SH_4	Customer Impersonation (N) Device Impersonation (SH) Message Modification(N) Replay attack(N) Repudiation(N)	Integrity Non repudiation Authentication	L-H
SH_5	Customer Impersonation(N) Eavesdropping/Message(N) Interception (N) Message Modification(N)	Confidentiality Integrity Authenticity	L-M

Existing studies of smart home security

The internet of things is a relatively new thing in the world of technology today. However, the Internet of things is predicted to be an extraordinary trend in the future. In this section, the previous works related to the security and privacy in the smart home are looked into. Security and privacy applications. Other works are classified into small categories according to the security activities and efficiencies in smart home systems based on IoT. These works focus on security systems and applications for smart homes using IoT [14] [15] [16]. Secure data management in various devices, security enhancement in smart home systems and applications [17], and network system security and privacy control for home intelligence and IoT devices [18].

Other works discuss secure healthcare architecture and communication of nodes in a Constrained Application Protocol (CoAP; an application layer protocol that is prepared for use in Internet devices in IoT smart homes, such as wireless sensor network nodes) network [19], as well as security challenges between heterogeneous devices and different applications in smart homes [7]. Some studies focus on password security and applications for IoT smart home systems [20] [21], secure software updates in smart home devices, and security system devices (e.g., surveillance cameras) and their use in smart homes [22]. Home automation and security threats are also defined, A new solution is presented to address risk reduction in cases of privacy breaches in smart energy management systems [23]. The work of [24] suggested the use of Radio Frequency Identification (RFID) tags for successfully identifying various items inside a smart refrigerator. This technique could be extrapolated to improve home security, but it requires most items inside the home including home inhabitants fitted with RFID tags, which is inconvenient and difficult to implement considering forgetful human nature.

privacy-enhanced security architecture proposed by [8] is applied in a smart home environment. architecture has a defense against such attacks as personal information hijacking and burst attack between an attacker and devices in a smart home environment. The study proposed a security framework applicable to a smart home environment, which includes encryption, access control, digital signature, authentication, and logging. the framework proposed [25] is based on the open source framework 'AllJoyn'. It is comprised of device, AllJoyn Core, permission module, and ACLs and policy certificate trust anchor. In the framework, critical data are transmitted after authentication between devices. End-user's security manager provides security provisioning and maintenance service for devices. A session is established between the applications of devices for data transmission. Authentication is performed with the use of a group key and a certificate. Authenticated devices transmit the messages encrypted with a given policy. [8] uses the authentication process of smart devices and lightweight lattice-based homomorphic cryptosystem to encrypt a message. It is divided into the initialization phase and reading aggregation phase. Since the scheme makes it possible to monitor authentication between smart devices, control center, smart meter, and communication between APs, the control center can decrypt an encrypted message to improve confidentiality and privacy of devices. To authenticate smartphones and send messages safely in a smart home environment, [26] uses an encryption algorithm and a hash function. The algorithm applies AES256, ephemeral Diffie-Hellman key exchange, and RC4-based hash function. With the use of a central hub, all messages to transmit are monitored, and the messages sent by smartphones pass the central hub for transmission. A message to transmit is encrypted with three algorithms, and a hash value is generated.

In 2014, the view of the Internet of things has evolved along with the development of technology and the incorporation of several technologies, ranging from wireless communication to the Internet, and from embedded systems to micro-electromechanical systems (MEMS), this means that all fields in the world will contribute to building the Internet of things [3].

Although many benefits are gained from IoT-based smart homes, these smart homes are susceptible to different attacks [27]. An individual can directly attack an interconnection device (e.g., gateway) or field device using its network or local communication interface (i.e., attacking the device) and a device can be impersonated using its faulty certificate. Household appliances can be connected to a wired or wireless network via the home gateway. An attack against the home

gateway can immediately lead to an attack against the whole household network, as it is the point at which an outside connection can be made [28].

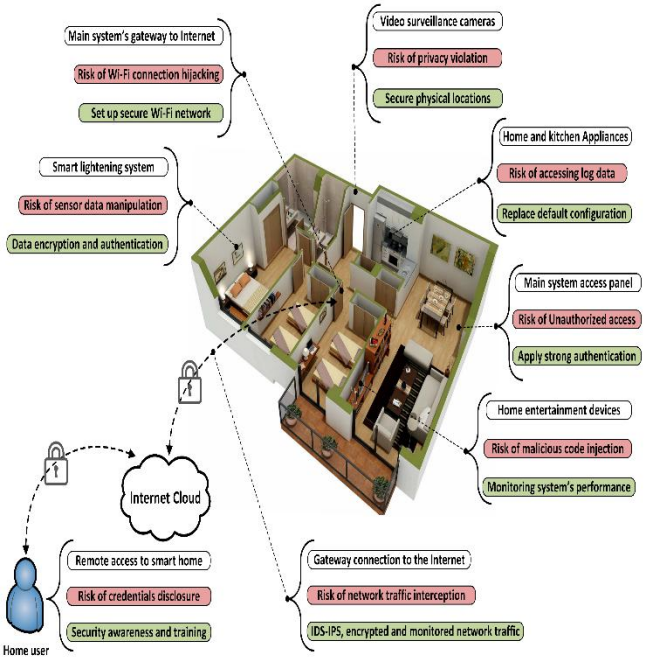

Figure 2. Security risks and mitigation approaches are pointed to an actual smart home environment. The floor plan was borrowed from Amazing Architecture [28].

IoT-based smart home architecture is split into three layers; device or perception layer, network layer, and applications layer. Figure two represents a typical IoT-based smart home environment and shows the known security risks and their corresponding countermeasures mapped to the smart home environment. Security risks will cross over one IoT layer. for instance, the risk of unauthorized access is found in accessing the main system configurations, accessing the IoT gateway, and within the login to the smart home applications. Therefore, a robust authentication method needs to be enforced in all those points. biometrics technology is embedded in multi-factor authentication to build a strong user authentication mechanism [29].

3. RESULT AND DISCUSSION

The security system in the Smart Home environment is a system that can help security officers and residents of the environment to be able to monitor the surrounding environment. This is in minimizing the possibility of criminal interference both from outside the environment or from within the environment itself. The smart home itself is one branch of ubiquitous and pervasive computing. Smart Home offers a more practical quality of life by introducing automation of household appliances and household assistants. Automation is based on a context-aware obtained from the results of monitoring the home environment itself. Users can control their home appliances remotely, for example when the user is still on his way home, he is able to turn on the air conditioner to cool the room, control the water heater for bathing and so on.One of the security problems on IoT devices is that the default password on the device cannot be easily changed by the user. This allows a hacker to control the device in a DDoS attack. The software used to control the device is a package of malware named Mirai. The source code for the software was distributed to the public earlier this month, although the perpetrators are still unknown. Mirai malware itself was first introduced by a hacker named Anna-senpai on a hacker forum. Since then, Mirai is estimated to have infected millions of IoT devices around the world. One feared was that a DDoS attack by Mirai botnet returned and quickly crippled the internet. Moreover, Mirai is very difficult to track, so hackers will feel safer when using it. Girai is a botnet specifically designed to attack IoT devices, such as routers, CCTV cameras, to printers that are all connected to the Internet network. Mirai botnet can scan various IoT devices automatically. The target is an IoT device with a weak security system, especially devices whose username and password have not been changed [30].

Devices infected by Mirai will continue to look for IP addresses from other IoT devices even though they are connected on the Internet network. There is an exception list of IP addresses that will not be infected by Mirai including the private network and IP addresses of several departments in America and certain companies. After successfully finding the IoT device that was the target, Mirai then waited for an order from the hacker to be activated. Once activated, Mirai will send an anonymous data packet to the server that is the target of the attack. The data package is indeed small, but if it is sent by hundreds of millions of IoT devices simultaneously, the result will be a DDoS attack that will not be blocked. There are hundreds of thousands of IoT devices that use default settings, making them vulnerable to infection. After being infected, the device will connect to the command and control server that shows the target of the attack.

The Mirai attack can be anticipated by rebooting the system. However, experts stated that rebooting did not eradicate Mirai, only holding back attacks for a while. Because in a matter of minutes, Mirai can deploy his troops again. Another option to stop Mirai attacks is to change the default password on IoT devices. The Mirai maker stated that this botnet was made in anticipation of the high-security awareness of various institutions. With the increasing level of security awareness, it was blamed

Besides Mirai and key installation (KRACKs), there is also a Bricker Bot attack. Bricker Bot made the news a few weeks ago because it was responsible for tapping an unsecured IoT device offline, rather than hijacking it to another botnet and using it for DDoS attacks like the big event seen last year against DYN. This is the third botnet that targets unsafe IoT devices, but the only one that is destructive. The second, dubbed Hajime, breaks IoT devices, but instead of bricking, they disable remote access to devices from the internet. Of course, Mirai is the first, but has the same goal as other botnets, namely to enslave IoT devices and use the computational power of the collection of bots for anything that might please the threat actors behind it. While a Bricker bot might not be a worm with mass adoption, it could be a precursor of things to come. It has all the initial indications of potentially very dangerous (even more than now) because it gets more appeal. There are millions of unsecured devices just waiting for someone to hijack them, with hundreds of thousands coming online every day. Because so many of these devices have little security, they pose a serious risk to the digital economy.

As have seen, because of its widespread deployment, mobilizing them to engage in attacks such as a large DDoS attack last fall, almost certainly will bring a large portion of the Internet to the cessation of grinding, disrupting business, affecting services, and potentially impacting critical infrastructure [31].

Bricker bots are different because they only deactivate the ability of IoT devices to connect to the Internet. If vendors are not interested in ensuring that they send secure devices by default, and if the owner doesn't care about security, it is only a matter of time before the device is violated and part of So botnets to warn the market about this problem, Bricker both authors choose to knock them offline [32].

To overcome various IoT security threats in the smart home environment, the first thing that can be done is to stop using the default password from the device and then deactivate remote access (WAN) to the computer device. With the onset of IoT device users, the two principles above must be the basic norm for running IoT devices. Over the past few years, many antiviruses have developed signatures and other detection techniques to inhibit botnet growth. Therefore to make a botnet that is not detected by antivirus is not an easy thing. From this argument, it can be said that IoT security in the Smart Home environment is quite good and this can be improved by using a special username and password to avoid hackers in the future.

Smart Home obviously emerges, positioning as the most noteworthy Internet of Things application on every deliberate channel. More than 60,000 individuals as of now look for the expression "Brilliant Home" every month. This isn't an astonishment. The IoT Analytics organization database for Smart Home incorporates 256 organizations and new companies. A larger number of organizations are dynamic in the savvy home than some other application in the field of IoT. The aggregate sum of subsidizing for Smart Home new companies as of now surpasses $2.5bn. This rundown incorporates noticeable startup names, for example, Nest or AlertMe and additionally various multinational enterprises like [33].

With such a significant number of players required with the IoT, there will undoubtedly be progressing turf wars as inheritance organizations look to secure their restrictive frameworks points of interest and open frameworks defenders endeavor to set new gauges. There might be numerous norms that develop in light of various prerequisites controlled by gadget class, control necessities, abilities, and employment. This presents open doors for stage sellers and open source backers to contribute and impact future models [34].

The privacy and security issues, as the IoT associates more gadgets together, it gives more decentralized passage focuses on malware. More affordable gadgets that are in physically traded off districts are more subject to alter. More layers of programming, combination middleware, APIs, machine-to-machine correspondence, and so forth make greater multifaceted nature and new security dangers. Hope to see various procedures and merchants tending to these issues with arrangement driven ways to deal with security and provisioning. With remote sensors and observing a center utilize case for the IoT, there will be elevated affectability to controlling access and responsibility for. Compliance will keep on being a noteworthy issue in medicinal and helped living applications, which could have life and passing repercussions. New consistency systems to address the IoT is special issues will develop. Social and political worries around there may likewise frustrate IoT appropriation.

4. CONCLUSION

Internet of Things (IoT) applications which will greatly affect human life. The IoT applications will go from a brilliant home to keen human services with propelling innovation. IoT Applications very important to be a concern. The general public needs new, adaptable, perfect and secure answers for both the administration of the always wide, unpredictably arranged Internet of Things and furthermore for the help of different plans of action. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. The security requirements are confidentiality, integrity, and authentication. Based on the data survey, there are different types of attacks are categorized as low-level attacks, medium-level attacks, high-level attacks, and extremely high-level attacks along with their nature/behavior as well as suggested solutions to encounter these attacks are discussed. Considering the importance of security in IoT applications, it is really important to install security mechanism in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networks.

More sensitive information has been collected, transferred and used by IoT devices especially smart home and healthcare devices, which inevitably involves more privacy problems. New IoT devices and protocols are more likely to contain potential vulnerabilities, which catching more efforts to solve these problems. The leading cause of insufficient security configures and vulnerable cloud and web service is the lack of security awareness as mentioned above. In addition, although security research on IoT operating system and mobile application are less in the past years,

more attackers will find and use the potential system and application vulnerabilities in future due to the "constrained" and "interdependence" IoT features. These findings motivate several recommendations for device designers, researchers, and industry standards to better match device privacy features to the expectations and preferences of smart homeowners.

5. REFERENCES

[1] T. K. Priyambodo and Y. Prayudi, "Information security strategy on mobile device based egovernment," ARPN J. Eng. Appl. Sci., vol. 10, no. 2, pp. 652–660, 2015.

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

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

[4] S. Yoon, H. Park, and H. S. Yoo, "Security Issues on Smarthome in IoT Environment," Springer, Berlin, Heidelberg, 2015, pp. 691–696.

[5] A. M.-2014 I. I. C. on Distributed and undefined 2014, "Cybersecurity for personal medical devices internet of things," computer.org.

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

[7] C. Lee, L. Zappaterra, Kwanghee Choi, and Hyeong-Ah Choi, "Securing smart home: Technologies, security challenges, and security requirements," in 2014 IEEE Conference on Communications and Network Security, 2014, pp. 67–72.

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

[9] A. Jose, R. M.- SmartCR, and undefined 2015, "Smart home automation security," researchgate.net.

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

[11] S. Chitnis, N. Deshpande, and A. Shaligram, "An Investigative Study for Smart Home Security: Issues, Challenges, and Countermeasures," Wirel. Sens. Netw., vol. 08, no. 04, pp. 61–68, Apr. 2016.

[12] Y. Prayudi and A. Ashari, "A Study on Secure Communication for Digital Forensics Environment," Artic. Int. J. Sci. Eng. Res., 2015.

[13] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures," IEEE Commun. Surv. Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.

[14] 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.

[15] 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.

[16] 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.

[17] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob), 2015, pp. 163–167.

[18] I. Sanchez et al., "Privacy leakages in Smart Home wireless technologies," in 2014 International Carnahan Conference on Security Technology (ICCST), 2014, pp. 1–6.

[19] O. Bergmann, S. Gerdes, … S. S.-W., and undefined 2012, "Secure bootstrapping of nodes in a CoAP network," ieeexplore.ieee.org.

[20] 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. 1–6.

[21] 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 MapReduce Systems View project An IdM and Key-based Authentication Method for providing Single Sign-On in IoT."

[22] P. Rajiv, R. Raj, and M. Chandra, "Email based remote access and surveillance system for smart home infrastructure," Perspect. Sci., vol. 8, pp. 459–461, Sep. 2016.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] J. He, Q. Xiao, P. He, and M. S. Pathan, "An Adaptive Privacy Protection Method for Smart Home Environments Using Supervised Learning," 2017.

[28] B. Ali, A. Awad, B. Ali, and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," Sensors, vol. 18, no. 3, p. 817, Mar. 2018.

[29] S. H. Khan, M. Ali Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," Pattern Recognit., vol. 48, pp. 458–472, 2014.

[30] H. Lin, N. Bergmann, H. Lin, and N. W. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," Information, vol. 7, no. 3, p. 44, Jul. 2016.

[31] N. Azman and B. Masalah, "Perancangan Software Aplikasi Pervasive Smart Home," vol. 2009, no. Snati, pp. 1–5, 2009.

[32] R. H. Weber, "Internet of Things – New security and privacy challenges," Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, Jan. 2010.

[33] N. Jyoti, "Internet of Things (IoT) : Security, Applications, Challenges and Future Directions," 2017.

[34] M. Abdur Razzaq et al., "Security Issues in the Internet of Things (IoT): A Comprehensive Study," 2017.