JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
SICAIET
2024
Review Article
Collection: Artificial Intelligence and Emerging Technologies

A Review Study on Smart Homes Present Challenges Concerning Awareness of Security Mechanism for Internet of Things (IOT)

Muhammad Ramzan[1], Zia Ur Rehman Zia[2], Muhammad Kamran Abid[1*], Naeem Aslam[1], and Muhammad Fuzail[1]

[1]Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan.
[2]Department of Computer Science, Institute of Southern Punjab, Multan, Pakistan.
[*]Corresponding Author: Muhammad Kamran Abid. Email: kamranabidhiraj@gmail.com

Academic Editor: Salman Qadri **Published:** February 01, 2024

Abstract: With the Internet of Things, the internet's reach is extended to tens of billions of devices. Due to the diversity of connected items and their associated needs, establishing a solid basis for the Internet of Things and ensuring its security is becoming increasingly difficult. The Internet of Things (IoT) will raise a slew of serious security risks, according to experts. Widespread espousal of the Internet of Things may result in security and safety concerns due to the close connection that exists between the actual world and the Internet of Things. There is a need of developing a way for safeguarding devices that are contained within a set perimeter and a supple shield strategy for safeguarding the Internet of Things in a smart home. The study will present a high-level architecture of the gateway for providing better security and privacy to IoT.

Keywords: IoT Security; Smart Home; IoT privacy.

1. Introduction

With the Internet of Things, the internet's reach is extended to tens of billions. Due to the diversity of connected items and their associated needs, establishing a solid basis for the Internet of Things and ensuring its security is becoming increasingly difficult. The purpose of this thesis is to address the security and privacy concerns associated with IoT in the environment of smart homes. The first and most critical contribution is the creation of a gateway that acts as a barrier between the smart home and the rest of the world, between the house's gadgets, and external users such as service providers. It is capable of delivering authentication, authorization, privacy, and secrecy in an encrypted fashion. This is particularly true for restricted devices that are incapable of self-preservation. This approach incorporates security domains, and the architecture is easily extensible to add new methods. Moreover, the gateway is a service discovery, which is accomplished by identifying a device that provides the required services [1]. Security is enforced by the gateway depending on policies[2] set by the user. The present study includes a policy description language (with the extensive review of relevant studies) that was created specifically for this purpose[3]. It enables users to set criteria for their gadgets regarding communication routes with smart devices in and outside the home[2]. There is just a minor impact on performance, as demonstrated by the performance tests, which allow for tens of sessions setups per second and hundreds of communications to be exchanged per second within a session. As a result, the gateway provides a cost-effective method of providing Internet of Things security. In part because of the gateway's flexibility in supporting a variety of security providers

as well as its ability to address the state of operation, developers will be able to create secure applications for the diverse Internet of Things[4]. In recent years, the internet's reach has increased tremendously in scope.

The arrival (with the invention) of smart gadgets[5] connected to the internet will permit the next expansion of this scope. Several of them have recently been released on the market. Smart TVs are now in many homes, allowing families to not only watch TV but also to browse the web, view YouTube videos, and make Skype conversations, among other things[2]. Smart refrigerators, thermostats, and lightbulbs are some more examples. The introduction of smart devices[5] that connect to the internet will enable the next widening of this research. A number of them have recently been brought to the market [2]. While, Other examples are smart thermostats, smart lightbulbs, smart fridges, smart internet devices and so on[6] .

The Internet of Things (IoT) will raise a slew of serious security risks, according to experts. Widespread adoption of the Internet of Things may result in security and safety concerns due to the close connection that exists between the actual world and the Internet of Things. To gain entrance into the victim's home, a burglar may choose to use sophisticated technology rather than a crude tool such as a crowbar, depending on the level of protection that is there. As sensors collect and transmit data from every location where humans can be found, the need for privacy becomes increasingly apparent[7].

A considerable deal of everyday technology has already developed to the level of "smart" technology, as previously stated. On the other hand, it is undeniable that there are still certain security concerns. While the applications described in Section 1 are unquestionably interesting, the focus of this thesis is on the smart home scenario. This is true even while the feasibility of smart cities and smart offices is being researched. Because of the development of consumer-oriented gadgets, predictions indicate that by 2019, more than two-thirds of American households will own at least one smart device, according to the Federal Communications Commission[8]. Several variables, including those described above, will lead to a considerable increase in the number of Internet of Things (IoT) devices detected in low-tech households. While sensors, smart refrigerators, and smart TVs are all examples of equipment that will be essentially static in nature, smartphones and wearables will be mobile gadgets that will frequently enter and exit the home, as well smartwatches and jewelry. For example, a smart house will be comprised of a vast array of products, each of which will have its own set of traits and functionalities. Because of this, we may need to create new categories for smart home devices to identify them more properly going forward. In addition, when used in conjunction with other items, sensors that detect movement or presence while also monitoring physical phenomena such as temperature and humidity can be created. In contrast to the electrical actuator described above, a mechanical actuator, such as one that opens and closes doors and windows, does not operate in the same way.

With our study, it is hoped to contribute to the Internet of Things through developing a way for safeguarding devices that are contained within a set perimeter, such as the smart house described earlier. This node is in charge of keeping track of all Internet of Things communications and exchanges that take place between the protected domain and the rest of the world. The gateway is described as a device with adequate processing power and memory to perform significantly better than the average smart home item in terms of functionality and reliability. The hub can carry out complex security activities because of the large number of resources that are available[9].

Many different types of perimeter devices can be used to make them compatible with the Internet of Things and its diverse variety of products and services. Also implied by this is that we will make every attempt to provide support for devices that utilize the smallest amount of resources possible. For applications and developers to connect to these Internet of Things gadgets, a central hub should be

established. I think it's important to emphasize that one of the most important prerequisites for gaining this protection is the ability to set security and privacy policies and laws. People who are not technically savvy should be able to use this functionality with relative ease.

2. Literature Review

2.1 Issues with the IoT

It is still necessary to establish clear standards to combine the services given by objects created by different manufacturers, and here is where the most difficult issues arise. It is recommended that the addressing and identification of devices be considered a first-level sub problem. As a result, to go from a 64-96 bit RFID tag identity to a 128-bit IPv6 identity, for example, mapping device identification to (IP) addresses is required. It is critical to be able to discover devices quickly based on their characteristics or groupings. This goal may necessitate further development of the Item Name Server concept. Several researchers, like Wortmann and Flüchter[10], believe that device mobility within a network should be permitted as long as scalability and flexibility criteria are met. there is the issue of energy usage to take into consideration. Certain items are passive technology competent, which means that they can function without the usage of a battery to function properly.

2.2 Privacy and security

As previously stated in the introduction, strict security and privacy measures are required to protect sensitive information from unauthorized access. Rather than being a minor inconvenience, these misgivings are a significant hurdle to the widespread adoption of the Internet of Things. As a result of a large number of available devices, the first problem is created. Because many of them have limited financial means, it is difficult for them to implement significant security measures. Furthermore, because of their diversity, the objects are compatible with a wide range of security approaches and protocols. Furthermore, many of these gadgets do not have enough memory to perform their functions properly.

The expansion of the internet's reach is expected to result in the development of new threat models. The fuzzy nature of the "perimeter" in an IoT environment means that an attacker can be both within and outside of it at the same time, posing a threat to both. Furthermore, because many things are available to the general public and easily accessible, physical attacks may grow more common [11].

2.3 Security method & solution for the aforementioned security issues

Recent years have seen an increased focus placed on the importance of encryption as a security enabler. Asymmetric and symmetric variations of the algorithm are available for use in cryptography, with the former being the default. It is more convenient and resource-efficient to use the former method, but it has limitations in terms of scalability and crucial management considerations to consider. “Although the latter is more flexible and allows for key distribution, it has a negative impact on performance as a result of this. Given the limitations of available resources, it has been investigated whether or not effective encryption in software is practical. A hardware implementation of the symmetric AES-128 was tested against software implementations of AES-128 (both pure and optimized), as well as against other symmetric cyphers, on a CC2420 CPU. Hardware encryption provides a significant performance advantage over software encryption in terms of execution speed, but only a slight advantage in terms of memory consumption compared to software encryption”. If asymmetric techniques had been used, the program execution time would have been significantly longer. Fortunately, this was not the case[12].

Communications must be encrypted in order to maintain confidentiality; only the person who has access to the encryption key. You might review the encryption mechanisms that were previously described in the preceding section of this chapter to refresh your memory. The Leap+ system, which employs

symmetric keys to maintain message secrecy, is in charge of ensuring message privacy and confidentiality. Because it can only be utilized under static settings, it is only used in a limited number of cases, which provides it with a distinct advantage over other strategies in terms of efficiency. The situation is made worse by the fact that when nodes are taken while the process of forming pairwise connections is in progress, the entire network is at risk of collapsing. TinySec and MiniSec are only capable of maintaining secrecy when conversing over the connection layer of the network. When using the Transport Layer Security (TLS) protocol to encrypt and authenticate UDP connections, it is possible to keep the contents of such discussions private. The use of this technology at the global internet level safeguards data for individual datagrams. Using public key infrastructure and DTLS, it is possible to design an end-to-end security architecture for low-end devices; however, this system has not been proven on such devices. Customers of Sizzle may benefit from end-to-end encryption through the use of ECC (Encrypted Communications Center).

2.4 Personal privacy is important

Some authors also contend that the aims of privacy and security may be in conflict with one another and that a compromise must be made to resolve this issue [source]. Following the Privacy by design principles, no one should ever be compelled to choose between two opposing goals that are incompatible with one another. Instead, integration between the two goals is achievable. Certain security protocols have been implemented to safeguard the personal information of individuals. Anonymous authentication and authorization are made possible through the use of attribute-based solutions, which verify.

2.5 Policies

Although it is not explicitly created for the Internet of Things, it aims to promote more expressiveness in general. Remora is a component-based development framework that facilitates the building of sensor-based systems and other electronic devices. Even though this architecture provides abstractions for dependencies, it does not have any provisions for cybersecurity. A framework that is not particular to the Internet of Things. While the Architecture Analysis and Design Language (AADL) was developed specifically to define components in embedded systems, an additional language was developed for broader use.

Some scenarios involving the smart home are shown to illustrate normal smart home behavior and interaction between people and the technology. Getting in touch with other devices. A resident's location is captured by the system while she is travelling throughout the house, allowing the system to follow her movement across room and zone boundaries. “The identification of a resident may be accomplished by facial recognition, or the monitoring of a user identification device, such as a smartphone or an RFID tag worn by the resident, may be accomplished through location data. Demotics hubs receive data from sensors and relay it to them. This method makes use of the information collected to help the people who live in the area. To accomplish this, the smart home loads the user's preferences from the user's smartphone or the user's home sphere before the user's arrival. The system must verify that the input is reliable because identification and preferences have been positively confirmed”. The gateway sends the necessary instructions to the temperature control and lighting systems, which are subsequently executed under other criteria such as the time of day and the location of the gateway. This type of system must verify that the commands are genuine and authorized to prevent abuse. For example, if they are in disagreement with their neighbors, they should not be permitted to make changes to the heating system in such a way that the house becomes uncomfortably chilly.

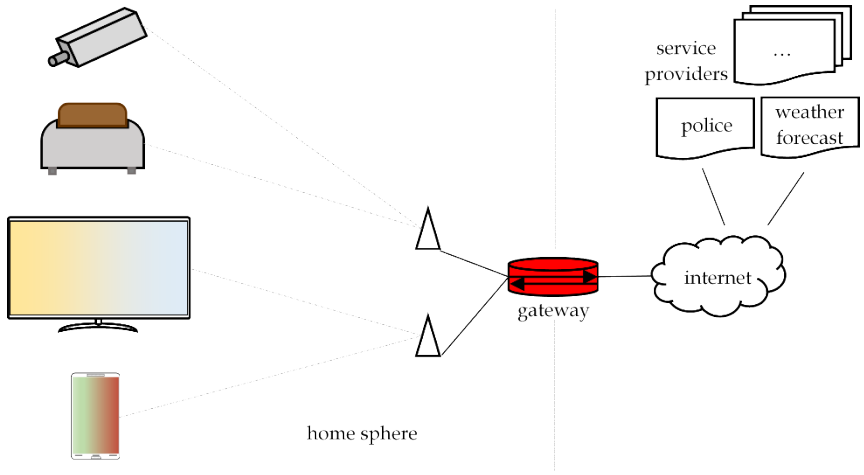

Figure 1. The smart home architecture

It should not be permissible for them to modify the heater to make the house overly cold, for example, if they are fighting with their neighbors. According to the participants in this debate. The system can reverse the alterations made to a room after everyone has left a facility in addition to readjusting rooms when a resident or guest arrives. The system turns off the lights and adjusts the heating so that it consumes the least amount of electricity possible.

3. An Overview of the Architectural Framework

According to the "high-level architecture of the gateway, it is comprised of three front-ends and seven inside portions. Likewise, both the Internet FrontEnd and the Home Sphere FrontEnd serve as a connecting point between the gateway and other networks on the Internet, as well as between the gateway and other networks inside and outside of the network, respectively. Through the provision of a proxy for their services and device interfaces, they can provide a communication interface for devices to interact with one another. These modules enable the establishment of sessions with entities both within and outside the smart home, as well as the transmission of communications such as orders from service providers or other devices. The result is that most normal gateway traffic entering the network passes through them as its principal point of entry. Config FrontEnd, on the other hand, provides users with the ability to make changes to the gateway's configuration, such as adding devices and users to the system, as well as changing access limits and other parameters. When it comes to the network's front-ends, the Network Manager is in charge of both internal and external interfaces to the network, which is both under his control". In other words, it converts IP addresses into more abstract entity representations that can be utilized by the gateway to communicate with other components of the system. When it comes to ensuring that security needs are met in a functioning manner, this module is the most important internal component to have. One approach to meet these requirements is by the enforcement of regulations for certain connections between an entity and a gateway, or between an entity and another entity, among other methods of meeting them. Following the guidelines, it is also responsible for identifying the most appropriate message security method for a session and for delivering the session key material that corresponds to that mechanism. More detail is provided in Section 4.3 on the topic of Enforcement, which encompasses a wide variety of capabilities and is composed of a huge number of submodules[13].

3.1 Scope of Use and Application

Third parties can connect to the gateway and use its features via remote sessions with service providers or residents. Service providers take advantage of public key infrastructure to the greatest extent

possible. As a result, an external contact system that is both scalable and versatile is created. Remote sessions can also be used to identify the remote device by utilizing public keys that are shared among participants. If the user's shared secret has previously been registered with the gateway, it may also be used.

3.2 Devices are classified.

Groups enable direct communication between groups of devices, eliminating the need for all communications to pass through the gateway. Certain constraints (policy) must be imposed on the formation of such a group. Following the group's formation, the gateway will be in charge of delivering critical information to all participants.

3.3 Session-level authentication

After authentication has been established using one of the procedures described above, authentication within a session will be required. If the message security requirements require confidentiality on the part of the entity, the system uses authenticated encryption to encrypt future communications provided to the entity. This ensures that the validity, integrity, and confidentiality of the data are all protected. After encrypted communications have been encrypted, they are authenticated. If the security of the communication requires authentication and integrity, regardless of whether the communication is secret or not, a message authentication code is generated and attached to each message to ensure its integrity. A shared session key will be required in both of these scenarios. This is generated and provided automatically by the system as part of the session setup operation.

4.Functional Specifications

fundamental functional need that happens in all usage situations dictates that the gateway should serve as an interface for the Internet of Things objects that are enclosed within the perimeter. As a result, it should provide an API that allows third-party apps and services to access the home sphere from the perspective of the web.

4.1 Consumers and Resources

There are two types of entities in terms of concept: resources and consumers. Resources are the type of entity that produces resources. When it comes to resources, everything that offers functionality counts, whereas a consumer is anybody who makes use of it. As a consequence, Consumers will submit instructions and requests to Resources, and Resources will reply with information and replies.

4.2 In a private environment, you can communicate with a gadget.

A secure channel may be established and maintained by some devices on their own, and as a result, they can authenticate and encrypt their communications without the assistance of a third-party gateway. Whenever interacting with such a device, users might elect to request a private session, which means that the security function of the gateway is being bypassed. As a result, a service provider might create a secure channel of communication with a home-sphere device to provide services. Consider the interaction between the “Energy Company and the smart meter, which is a device owned by the service provider but placed in the smart house, as an example of how this may work”[14].

4.3 Configuration

Expansion of the existing system by incorporating new devices and services. To illustrate this point, consider how adding a smart TV to the home sphere highlights how the gateway must be equipped to support the addition of additional devices to the home sphere. This functionality must be supported by the gateway for it to work. It may be necessary for the user to interact with the device, or the gateway may receive a network signal informing it that a new device has become accessible, after which additional

configuration steps by the user are required. To proceed, it is important to declare some device-specific specifications. To properly identify the device, it will first be essential to define the device's Resource and/or Consumer identities, as well as its name, which will be used to identify the item. In addition, the applicant is needed to provide certain security information to the company.

5. Conclusion

In this thesis, it was proven that a flexible protection strategy for securing the Internet of Things in a smart home setting may be implemented. First and foremost, a thorough review of the literature was conducted, with specific attention placed on challenges and associated solutions in the Internet of Things sector. Some security-related problems were discussed in greater depth after the discussion of networking and addressing difficulties because they are the most important for the design of this thesis. A few of the most important findings reached were the importance of a uniform security architecture as well as the necessity of a suitable key management system. A related piece of work presented numerous methods for dealing with sub problems such as cryptography and authentication, as well as a study of the description of security policy descriptions gateway runs on a device that is far more powerful than the average Internet of Things item, and it is capable of providing security for devices that are not properly capable of doing so on their own. The system makes use of the concepts of Resources, which are entities that offer services, Consumers, who are entities that consume those services, and communication channels, which are entities that connect these two entity types. Another addition that would enhance the user experience is the introduction of a graphical interface for specifying policies and configuring the gateway. Such modifications would need only a few isolated changes to the gateway. It is not dependent on the kind of data transferred and enables interoperability with a wide variety of security technology-based solutions. The ultimate result will be that it will be easier for developers to create secure, generic, and interoperable Internet of Things apps for smart homes.

References

1. S. Sepasgozar et al., A systematic content review of artificial intelligence and the internet of things applications in smart home, vol. 10, no. 9. 2020.
2. A. S. Lago, J. P. Dias, and H. S. Ferreira, "Conversational interface for managing non-trivial internet-of-things systems," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12141 LNCS, pp. 384–397, 2020, doi: 10.1007/978-3-030-50426-7_29.
3. A. Rayes and S. Salam, "Internet of things-from hype to reality: The road to digitization," Internet Things From Hype to Real. Road to Digit., no. October, pp. 1–328, 2016, doi: 10.1007/978-3-319-44860-2.
4. Z. Sisi and A. Souri, "Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things," Trans. Emerg. Telecommun. Technol., no. November 2020, pp. 1–18, 2021, doi: 10.1002/ett.4217.
5. J. Huang, X. Wu, W. Huang, X. Wu, and S. Wang, "Internet of things in health management systems: A review," Int. J. Commun. Syst., vol. 34, no. 4, 2021, doi: 10.1002/dac.4683.
6. B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," Concurr. Comput. Pract. Exp., vol. 32, no. 21, pp. 1–24, 2020, doi: 10.1002/cpe.4946.
7. Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in internet of things: A comprehensive survey," IEEE Access, vol. 9, no. August, pp. 113292–113314, 2021, doi: 10.1109/ACCESS.2021.3103725.
8. P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, "Internet of Things: Applications, security and privacy: A survey," Mater. Today Proc., vol. 34, pp. 752–759, 2019, doi: 10.1016/j.matpr.2020.04.737.
9. A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, "AEGIS: A Context-aware Security Framework for Smart Home Systems," ACM Int. Conf. Proceeding Ser., vol. 2, no. 1, pp. 28–41, 2019, doi: 10.1145/3359789.3359840.
10. F. Wortmann and K. Flüchter, "Internet of Things: Technology and Value Added," Bus. Inf. Syst. Eng., vol. 57, no. 3, pp. 221–224, 2015, doi: 10.1007/s12599-015-0383-3.
11. A. Kevin, "That ' Internet of Things ' Thing," RFiD J., p. 4986, 2010.
12. O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks," Int. J. Commun. Syst., vol. 23, no. 5, pp. 633–652, 2010, doi: 10.1002/dac.
13. C. P. Mayer, "Security and privacy challenges in the Internet of Things," Electron. Commun. EASST, vol. 17, 2009, doi: 10.14279/tuj.eceasst.17.208.205.
14. H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, no. March, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.