Open Access
Full Length Article

ORIGINAL ARTICLE

IoT Environment Security and Privacy for Smart Homes

Muhammad Kamran Abid[1], Mubshra Qadir[2], Shahid Farid[3], Mujahid Alam[4]

[1]Department of Computer Science, NFC IET, Multan, Pakistan
[2]Department of Information Security, The Islamia University of Bahawalpur, Bahawalpur, Pakistan
[3]Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan
[4]ICCC, Informatics Complex, H-8, Islamabad, Pakistan.

ABSTRACT

A network of connected things that can communicate and exchange data is known as the Internet of Things, or IoT. The number of these connected devices will be 38.6 billion in 2025 and devices are collecting data continuously from your location, contacts, calendar events, smart homes, health devices, etc. Several security and privacy challenges arise due to its heterogeneity and use. The identification of the challenges and issues is important for better security and privacy. The research will focus on the current issues and challenges with an available solution for a smart home context. An IoT Smart Gateway concept has been introduced for dealing with the most common issues and challenges by using a pre-train machine learning model at the smart gateway, which deals with consumers and resource policies separately.

Keywords: IoT, Smart Home, IoT Security and Privacy

Author`s Contribution
[1] Data analysis, interpretation and manuscript writing, Active participation in data collection, Conception, synthesis, planning of research, Interpretation, and discussion

Address of Correspondence
Shahid Farid
Email: shahidfarid@bzu.edu.pk

Article info.
Received: July 6, 2022
Accepted: November 17, 2022
Published: December 30,2022

Cite this article: *Abid MK, Qadir M, Farid S, Alam M. IoT Environment Security and Privacy for Smart Homes. J. inf. commun. technol. robot. appl.2022; 13(1):15-23.*

Funding Source: *Nil*
Conflict of Interest: *Nil*

INTRODUCTION

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 purpose of this research is to address the security and privacy concerns associated with IOT in an environment of smart homes [1]. With the emergence of smart devices 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 browse the web, view YouTube videos, and make Skype conversations, among other things. Smart refrigerators, thermostats, and light bulbs are some more examples the introduction of smart devices that connect to the internet will enable the next widening of this research. A number of them have recently been brought to the market Other examples are smart thermostats, smart light bulbs, smart fridges, smart internet devices, and so on [2].

A new phenomenon known as the Internet of Things refers to the connectivity of all types of items (or "things") to the internet, such as today's smart gadgets, across a network (IoT)[3][4]. According to this vision, the world-

wide information infrastructure (II) has been built on the internet, and in which they will link and interact to benefit. To support this architecture, a slew of technologies has been upgraded or merged into it, including identification, tracking, communication, sensors, and distributed intelligence. As a result, the Internet of Things will be comprised of a diverse range of devices with varying degrees of capability. This also indicates that some of the participating objects will be limited in terms of their available resources. It is unquestionably true that the contact between people and a variety of gadgets will have a significant impact on every day and professional life in the near future, as it will provide new and improved service options in the process. Many Internet-of-Things (IoT) applications are being considered, developed, and implemented, including smart manufacturing, intelligent homes, and workplaces (including smart cities), intelligent retail (including smart stores), improved logistics (including shipping and distribution), and transportation and distribution. Some of the issues and unresolved concerns related with the Internet of Things, such as security and privacy of the IoT devices. With the wide variety of IoT devices, there are security and privacy concerns. Without a framework that enables such devices to communicate and use information in a private and secure manner, new and developing IoT gadgets cannot meet user expectations and may drive consumers away[5].

The Internet of Things (IoT) will raise a slew of serious security risks, according to experts. IoT device sales are estimated to reach 41 billion in 2020, according to research conducted by the International Data Corporation in 2013. The Internet of Things differs from the traditional Internet in that a human element is not present[6][1]. A 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. Security is a major concern in the modern world regarding data of different devices[7]. A huge attack surface is produced by the fact that everything is wired and connected, including IoT devices, from refrigerators to sprinklers[8]. 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[9]. Customer perceptions of security vulnerabilities are not only real; they are also present in many of today's smart gadgets[10]. Although the services provided by IoT apps are incredibly helpful to consumers, preserving their security and privacy can be very expensive. To defend the Internet of Things, it is critical that protocols and networks be protected from compromise. Improvements in cryptography will be essential to accomplish this goal. Even though many of the devices have limited resources, the use of encryption, authentication, and access control is required to regulate the usage of many of the devices.

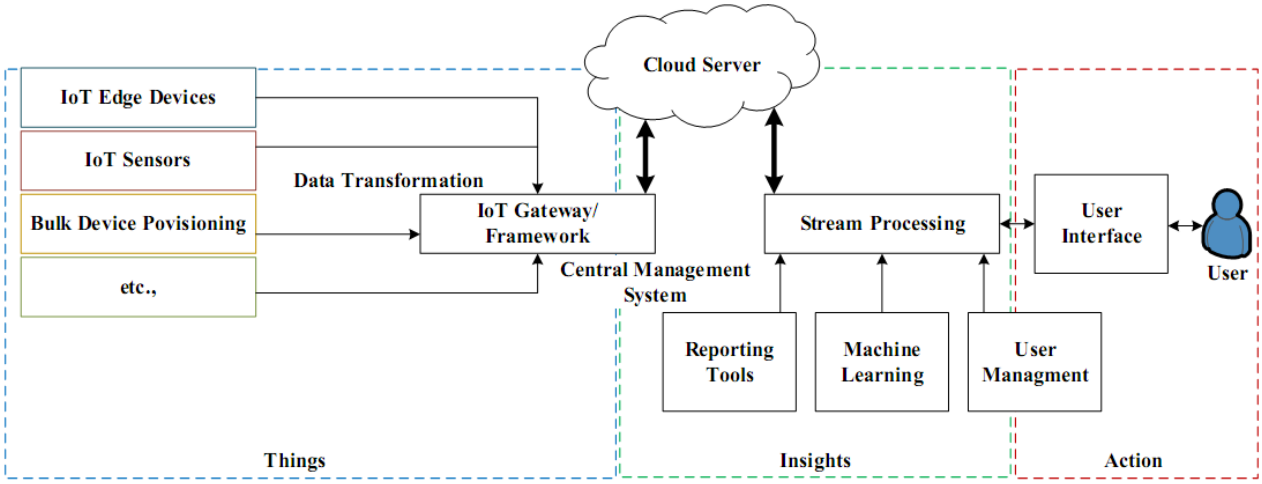

Figure1: Architecture of IoT[11]

In addition to security and privacy concerns, harmonization across a varied range of devices, protocols, and services represents a substantial problem that must be addressed. Despite multiple standardization efforts, many devices continue to use their own application-layer protocol for controlling them, even though several standardization initiatives have been conducted. 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. This node oversees keeping track of all Internet of Things communications and exchanges that take place between the protected domain and the rest of the world. IoT networks struggle with issues including privacy, authentication, storage, and data processing rates. Not to mention, IoT devices lack essential security software and modules and are simple in design. Cyber-attacks can be launched by criminals due to a lack of security.

LITERATURE REVIEW

The "smart home" category includes all network-connected light bulbs, outlets, door locks, door bells, home security systems, smart appliances, TVs, entertainment systems, thermostats, and smart appliances used in houses and buildings[12]. A computer or mobile device can be used to remotely control these Internet of Things (IoT) smart home gadgets through the internet. The "smart home" component of the IoT paradigm aims to combine security with home automation. By connecting common household items to the Internet, homeowners may remotely monitor and manage them. With features like time-controlled lights that turn off at specific times of the day and smart thermostats that regulate house temperatures and generate thorough energy usage data, smart homes have made a name for themselves in the consumer market[13]. The availability of affordable smartphones, microcontrollers, and other open-source hardware, as well as the growing use of cloud services, have enabled the development of low-cost smart home security systems[14]. The security and privacy of a smart home is main issues in the adaptation of modern technologies and getting there benefits[15][16].

A number of security issues are arising at different levels, these levels are divided into number of layers[17]. Normally the security of the IoT devices are divided into three layers, the Physical Layer, Network Layer and application layer[18]. Every layer has its own important regarding security and privacy[19], as the manufacturing companies are focusing less on the devices security due to low computation power and low energy consumption of the devices[20].Now we will discuss the IoT security issues with respect to different security layers.

Table 1: Security Issues at different layers

Security Issues at Physical Layer	Security Issues at Network Layer	Security Issues at application layer
Removing, destroying, or stealing IoT devices	Eavesdropping	Masquerade attack
Extraction of security parameters	Radio frequency jamming	Malicious code
Firmware replacement	Spoofing attacks	Trojan Horse
Node compromise	Interception attack[22]	Virus and Worms[21]
Malicious Node Injection[21]	Sinkhole Attack	Data corruption
Node capture Attacks	Sybil Attack	Sniffing attacks
Attack using false data injection	Traffic Analysis Attacks	Reprogram attacks
	Phishing site attack	
	Hello Flood attack	

The network design of the smart home poses the greatest security risk. Recent strategies for putting in place smart homes entail the ad hoc interaction of a wide variety of devices from many manufacturers. The smart home is exposed to a greater spectrum of risks due to this dynamic network design, which also greatly expands the attack surface area[23][24][25]. Three or five levels make up the layered architecture of the Internet of Things. The first three levels are physical, network, and application; the following five are physical, network, application,

middleware, and business. Threats and attacks against each layer's security are conceivable. Either of these options is possible. These risks could originate from both internal and external networks. The security of the IoT devices is not easy as compared to the simple IT devices as compared in table1.

Table 2. IoT security Vs Traditional IT Security	
IoT security	Traditional IT security
Security as built in Feature	Add-on Security
Lightweight algorithms	Complex algorithms
Security issues are due to auto collection of information	User control
Heterogeneity at large Scale	Heterogeneity at small scale
Only few security algorithms are available	Many security algorithms are available
IoT devices operate in open environments	IT devices operate in closed environments

Particularly regarding smart homes, traditional computer networks share many traits with them, including certain security concerns. On our home network, there might be hardware like PCs. smartphones and tablets with powerful processors they are often watched after by users and are powerful. On the other hand, IoT devices have hardware and design. Traditional security measures cannot be applied because of limitations[26][27]. The new techniques are needed for the security and privacy protection of the IoT devices like Machine Learning, Artificial Intelligence, and the future research is focusing on the New techniques to handle these issues[28]. Most of the security and privacy issues can be easily solved by using modern machine learning techniques[29][30][31].

Unbelievably large amounts of personal data and private information may be kept by a third party[23]. This becomes another major Security issues of the modern IoT devices. We will be most concerned with securing all of these connected devices[32]. More and more connections are being made between devices. Hardware, software, and connections must all be secure for Internet of Things (IoT) devices to operate successfully. The IoT's ability to expand could be hampered by any of these security concerns. Privacy is another concern regarding the IoT devices data. t is essential to ensure that the data is secure and only accessible to those who are authorized. Access to sensitive information is restricted to those who have been given permission[33]. A confidentiality breach occurs when someone has access to information they shouldn't.

To remotely manipulate a victim's machine and propagate malware, a "botnet"—a network of interconnected systems—is employed. Cyber-attacks like DDoS and phishing, as well as the theft of sensitive data and the gathering of online banking information, are all carried out using command-and-control servers. Cybercriminals can use botnets to attack Internet of Things (IoT) devices that are linked to a range of other devices, such as laptops, desktop computers, and smartphones[34].

By issuing numerous requests, a denial-of-service (DoS) attack overtaxes the resources of the target system. Instead of stealing crucial information, the attackers want to harm a company's brand and decrease income.

An attempt is made to break through the communication link between two different systems in a Man-in-the-Middle (MiTM) assault to intercept messages being transmitted between them. Attackers take over their communication and deliver bogus messages to the involved systems, which severely destabilizes them. It is important to validate authentication and the integrity of the software on the device using cryptographic hash algorithms, which generate digital signatures[21]. Unauthorized access to the sensor nodes can be prevented using point-to-point encryption and authentication techniques[21].

2.1. General Security Issues

- No clearly defined boundaries
- Devices are highly heterogeneous.
- No need of permission to installation like smart phone applications
- an unreliable web interfaces.
- Insecure cloud interface
- Insecure security configuration
- Poor physical security

RESEARCH METHODOLOGY

A thorough investigation has been conducted by identifying the key privacy and security concerns. In order to identify potential future problems with smart home IoT devices, the most recent literature has been taken into account. The various issues that have emerged as the biggest obstacles to the adaption of future IoT devices are identified. The major security and privacy challenges have

then been effectively addressed by a theoretical model. The model may separate the local network from the external network, ensuring the security and privacy of the smart home.

PURPOSED SOLUTION

To resolving security challenges, the concept of consumers and resources has been applied. The IoT smart gateway has been theoretically suggested as the solution for the local level network of a smart home.

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. Consequently, Consumers will submit instructions and requests to Resources, and Resources will reply with information and replies. The Gateway must act smartly, the rules and policies for Consumer-gateway are different and policies for Resource-gateway will be different. A IoT smart Gateway can handle these policies effectively and continuously update the policies automatically by using any machine learning prediction model.

4.2. Security and privacy Through IoT Gateway

A theoretical model that was proposed composed of an IoT Smart Gateway model which will be implemented at the border of a smart home sphere. An IoT gateway, a potent network processor, and the additional Internet of Things endpoints share the same local area network. In addition to being managed by a single central administration point, the coordination of IoT devices can enhance the connectivity and interoperability of smart devices. By numerous producers. Additionally, it might serve as a link between the nearby IoT infrastructures. Extreme computation Due to the gateway's increased resources and processing power, IoT devices can offload memory-intensive operations to the gateway. To prevent unauthorized access to or alteration of restricted data, the gateway provides access control and centralizes user authentication. It also functions as a firewall to safeguard data and smart devices while reducing attack surfaces and cyber security concerns.

The service platform, smart devices, home gateway, and home network are the four components of a smart home[35]. Many interconnected devices automatically share information over a home network in a smart home. To manage the information flow between smart devices connected to the external network, a home gateway was developed. A service platform makes use of a service provider's offers to deliver various services to the home network. The gateway offers an affordable approach to provide security for the Internet of Things. Developers will be able to produce secure applications for the wide variety of Internet of Things thanks in part to the gateway's flexibility in supporting several security providers as well as its capacity to address state of operation. The gateway must provide access to the services provided by the protected devices by providing control interfaces to the protected devices. As a result, the gateway should be capable of supporting users in the establishment of secure communications between devices using pre-configured configurations. The figure2 showed beforehand, the entryway remains between the external organization (web) and within home circle organization. In this manner, messages entering and leaving the home circle go through the passage. Moreover, correspondence between home circle gadgets additionally goes through the entryway, to such an extent that it turns into the main issue for really looking at security. The figure3 represent the concept of IoT smart gateway, as gateway act like a bridge for IoT devices to external internet/cloud. The simple gateway just implements the basic set of rules/policies, but the smart gateway uses a machine learning model to detect any malicious request by using its pretrained model. As the gateway has not such a computational power to run any machine learning model from the start, already train model can be used and these are called pretrained models.

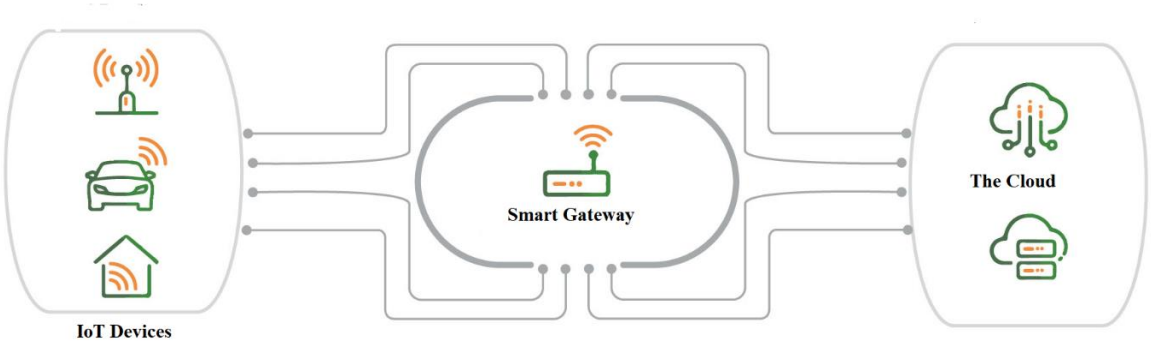

Figure2: IoT Smart Gateway

The pretrained model has develop on the large dataset and weights are to be adjusted, by using the weights of large data set a smart gateway can easily identify any new malicious request to the outside of home network.

A number of issues regarding security and privacy can be easily resolved. The gateway rules and policies are only for the known issues but in the modern day every day devices have to face some new kind of issue. So, gateway needs the power of prediction for the solution of any new type/unknown request. The pretrained machine learning model can be easily run on the smart gateway that can predict any malicious attack on the network and by blocking that issues the policies are automatically updated.

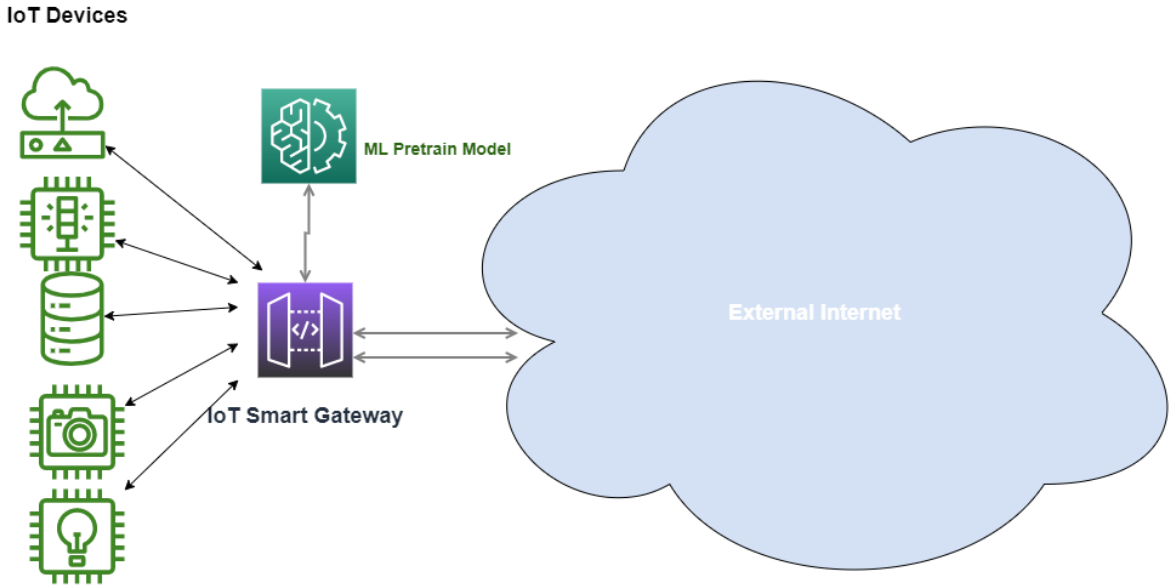

Figure3. IoT smart Gateway using pretrained model.

4.3. Issues to be resolved.

Several issues can be resolved, or their impact can be minimize using the ML pretrain model. This model will be train on a well-known issues dataset as the IoT smart gateway has no processing power to train the model from scrap level. This will use the previous train model and make predictions regarding current issues. The gateway is working on the policies and rules which are defined already, but the pretrained model will auto update the policies and rules using the pretrained prediction model.

The main issues to be resolved by using pretrain model are given below.

4.4. Denial of service

If the hacker is trying to access some IoT devices in a same manner from different resources, the model predicts as a malicious attack and block that request and update the policies of IoT smart gateway. Most of the attacks will be blocked automatically.

4.5. Botnets

A defined policies are not enough to tackle the phishing attacks using the botnets, but a smart gateway can predict the chances of phishing attack and block that request easily. At the same time the policies of gateway are also updated.

The smart gateway can protect a home area network from the outer malicious network traffic, but the rules and policies need to be continuously updating, there is also need of updating of that used pretrain model also. The major focus will be on the security of smart home buy securing it from the outside network. This will also provide the privacy to the IoT devices used in a smart home. But still this single model is not enough to handle all the security and privacy issues.

CONCLUSION

There is a need of flexible protection strategy for securing the Internet of Things in a smart home which can deals many securities relevant issues effectively. Several security issues are identified after the literature review with respect to different layers of IoT devices security. Some security issues are specific to the layers, and some are the general security concerns. All the issues have equal importance in the adaptation of IoT devices for the smart home context. The most of security and privacy issues can be resolved by managing the home area network as a private area network with respect to the external Internet. But on the other hand, the devices cannot be used effectively without the external internet, so there is need of a secure bridge between the personal area network and the external resources of the internet. The design of the gate, which is placed at the border of the home sphere and helps to protect it from invaders, that's called the IoT smart Gateway. The IoT Smart Gateway runs on a device that is far more powerful than the average Internet of Things item, and it can provide 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. Consumers often request that a Resource create an account with them, after which session material is established and any sort of raw data may be provided in regular messages through the gateway as part of the normal mode of operation, the Consumer-gateway and Resource-gateway sub channels can each be protected by a different security mechanism. A machine learning based pretrain model has been used to predict and update the policies for consumer & resources IoT smart gateway effectively. A number of security problems can be easily identified, and their effect can be minimized by using the Machine learning based pretrain model, which is train on any other dataset at any other powerful processing machine. But on the other hand, still there is need of full artificial intelligence-based system which can identified the security and privacy issues more effectively.

IoT Future

The safety of user data and privacy has been identified as one of the main problems with the Internet of Things. Consumer anxiety over privacy concerns is allegedly one of the major factors limiting IoT user adoption and one of the important factors impacting the success of the technology. Privacy issues are given top emphasis in the IoT ecosystem. A user's device is accessible to everyone, which puts their personal information at danger. There are two methods for dealing with privacy concerns. At first, the user's device rejects the request for personal data. Second, offer a network architecture that shields protected data from attackers and only permits the use device to return the desired data. It is necessary to have devices for user authentication, decentralized privacy mechanisms, privacy policies, and security and privacy profiles. Privacy needs to be more attention for the adaptation of the IoT devices in near future.

REFERENCES

1. E. A. Affum, K. A. Agyekum, C. A. Gyampomah, K. Ntiamoah-sarpong, and J. D. Gadze, "Smart Home Energy Management System based on the Internet of Things (IoT)," vol. 12, no. 2, 2021.
2. H. Niranjan, N. Mittal, and P. Hegde, "SMART AND EFFICIENT HOME AUTOMATION SYSTEM USING IOT," no. 3, pp. 3–8, 2021.
3. S. Akbar, K. T. Ahmad, M. K. Abid, and N. Aslam, "Wheat Disease Detection for Yield Management Using IoT and Deep Learning Techniques," vol. 10, no. 3, pp. 80–89, 2022.
4. S. Vashisth, S. K. Chawla, B. Mahjan, and H. Chugh, "INTERNET OF THINGS FOR SMART ENVIRONMENT APPLICATIONS," vol. 19, no. 5, pp. 417–434, 2020.
5. X. Liang and Y. Kim, "A Survey on Security Attacks and Solutions in the IoT Network," pp. 853–859, 2021.
6. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," vol. 4, no. 5, pp. 1250–1258, 2017.
7. M Kamran Abid, "An Analysis of Cloud Computing Security Problems," Int. J. Inf. Syst. Comput. Technol., vol. Vol. 1 No., no. 05-07–2022, 2022, [Online]. Available: https://ijisct.com/index.php/ojs/article/view/14
8. S. Millar and R. Llc, "IoT Security Challenges and Mitigations : An Introduction," pp. 1–5.
9. J. M. Blythe, S. D. Johnson, and M. Manning, "What is security worth to consumers ? Investigating willingness to pay for secure Internet of Things devices," Crime Sci., pp. 1–9, 2020, doi: 10.1186/s40163-019-0110-3.
10. R. El-azab, "Smart homes : potentials and challenges," no. January, pp. 302–315, 2021, doi: 10.1093/ce/zkab010.
11. A. C. Survey, "SS symmetry Internet of Things and Its Applications :," pp. 1–29, 2020.
12. L. W. Santoso, R. Lim, and K. Trisnajaya, "Smart Home System Using Internet of Things," vol. 16, no. 1, pp. 60–65, 2018.
13. M. A. Hoque and C. Davidson, "Design and Implementation of an IoT-Based Smart Home Security System," vol. 7, pp. 85–92, 2019.
14. V. S. Rao, "Internet of Things (IoT) based Home Automation System (HAS) Implementation of Real-Time Experiment," vol. 9, no. 11, pp. 200–204, 2021.
15. A. Ahmed, A. I. Abdulla, A. S. Abdulraheem, A. A. Salih, and M. A. M. Sadeeq, "Internet of Things and Smart Home Security Internet of Things and Smart Home Security".
16. E. Summary, "HC3 : Analyst Note HC3 : Analyst Note," pp. 1–4, 2022.
17. F. Kuntke and S. Linsner, "LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios," no. September 2021, pp. 1–20, 2022, doi: 10.1002/ett.4452.
18. T. Yashiro, S. Kobayashi, N. Koshizuka, and K. Sakamura, "An Internet of Things (IoT) Architecture for Embedded Appliances," pp. 314–319, 2021.
19. S. Nagarkar, "Evaluating Privacy and Security Threats in IoT-based Smart Home Environment," vol. 14, no. 7, pp. 75–78, 2019.
20. R. Venkatesan and M. V. Raghavan, "Architectural Considerations for a Centralized Global IoT Platform," 2015, doi: 10.1109/TENSYMP.2015.14.
21. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things : Security Vulnerabilities and Challenges," pp. 180–187, 2015.
22. Z. A. Almusaylim and N. Zaman, "A review on smart home present state and challenges : linked to context-awareness internet of things (IoT)," Wirel. Networks, vol. 5, 2018, doi: 10.1007/s11276-018-1712-5.
23. F. Hall and L. Maglaras, "Smart Homes: Security Challenges and Privacy Concerns," Int. J. Comput., vol. 14, no. October, 2020, doi: 10.46300/9108.2020.14.5.
24. S. Kousalya, G. R. Priya, R. Vasanthi, and B. Venkatesh, "IOT Based Smart Security and Smart Home Automation," vol. 7, no. 04, pp. 43–46, 2018.
25. A. W. Services, "Securing Internet of Things (IoT) with AWS," 2021.
26. C. Jo, P. Barros, and M. Tavares, "Vulnerabilities in IoT Devices for Smart Home Environment," no. Icissp, pp. 615–622, 2019, doi: 10.5220/0007583306150622.
27. T. Smart, H. Automation, and E. Paradigm, "Edge-Computing Paradigm," 2021.
28. S. Ahmed, "IoT Based Smart Systems using Machine Learning (ML) and Artificial Intelligence (AI): Vulnerabilities and Intelligent Solutions," no. Icsit, pp. 56–61, 2022.
29. E. Bout et al., "How Machine Learning changes the nature of cyberattacks on IoT networks : A survey to cite this version : HAL Id : hal-03390359 How Machine Learning changes the nature of cyberattacks on IoT networks : A survey," 2021.
30. I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence : A Comprehensive Overview, Machine Learning Solutions and Research Directions," no. March, 2022, doi: 10.20944/preprints202203.0087.v1.
31. A. S. Approach, "Security Requirements for the Internet of Things :," pp. 1–35, 2020, doi: 10.3390/s20205897.
32. B. K. Sovacool, D. D. Furszyfer, and D. Rio, "Smart home technologies in Europe : A critical review of concepts, benefits, risks and policies," Renew. Sustain. Energy Rev., vol. 120, no. December 2019, p. 109663, 2022, doi: 10.1016/j.rser.2019.109663.
33. A. Yacob, Z. Baharum, N. Aziz, and N. S. Sulaiman, "A Review of Internet of Things (IoT): Implementations and," no. December, 2020, doi: 10.30534/ijatcse/2020/5891.32020.
34. R. Ranjisha, "IOT SECURITY : CHALLENGES AND FUTURE TRENDS," 2021.
35. Z. Shouran and A. Ashari, "Internet of Things (IoT) of Smart Home : Privacy and Security," vol. 182, no. 39, pp. 3–8, 2019.