ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 11, Issue 4, pp: (43-50), Month: October 2023 - December 2023, Available at: www.researchpublish.com

Functions of Smart Security Using the Internet of Things-A Study

KSHITIJ NAUTIYAL[1], RAJEEV KUMAR[2]

Assistant Professor, Dept. Of Electrical Engineering. Dev Bhoomi Uttarakhand University, Dehradun[1]

Assistant Professor, Dept. Of Electrical Engineering. Dev Bhoomi Uttarakhand University, Dehradun[2]

DOI: https://doi.org/10.5281/zenodo.10255306

Published Date: 04-December-2023

***Abstract*: The Internet of Things (IoT) describes the network of physical objects— "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 22 billion by 2025. a significant number of Internet-connected devices generate massive amounts of data. The main difficulty in the IoT market is** Protecting **IoT devices and network data. Privacy, confidentiality, integrity, and dependability problems must be addressed while transferring user data across devices. This research analyses the communications action of IoT devices and mobile apps, security threats to IoT technology, IoT tools, manufacturers, and simulators. This article deals also with the role of the Internet of Things in advancing smart security.**

Keywords: **Internet of things, Smart Security Analyses.**

1. INTRODUCTION

Computer networking has advanced greatly in the age of wireless communication and interconnectivity. The "Internet of Things" was invented in 1999 by Kevin Ashton [1]. IoT is a new technology that links physical and digital items [2]. IoT devices, spanning wearables to industrial equipment, possess the capability to independently sense and take action. [3,4]. The expanding use of IoT apps in various industries unlocks more device accessibility. For instance, a company specializing in wearable tech monitors health and behaviors. Patients benefit from employing IoT apps and gadgets for personalized health insights. [5]. The "smart house" IoT includes smart refrigerators, heating, gardening, video doorbells, personal assistants for smart lighting, coffee makers, and door locks. Smart city uses and IoT devices include street lighting, garbage management, and parking [6]. Researchers are exploring IoT security. IoT security has garnered academic attention [7–13]. The essence of IoT's hurdles resides in data transit, collection, and robust security measures. These devices serve diverse tracking purposes, demanding specialized protocols for seamless data transmission. Overlooking these protocols exacerbates identity, permission, and security issues within IoT ecosystems. Login vulnerabilities pave the way for menacing cyber threats such as DDoS and password guessing attacks. Authentication across intricate networks amplifies the complexity, while protocols need to navigate device constraints like memory, energy, and computing capabilities for efficient IoT operations. [14–19]. Mishra et al. [20] studied IoT use, development, and obstacles. Layered IoT security challenges. IoT security was improved by comparing anomaly detection to the newest IDS. According to Hameed and Alomary [21], authentication and lightweight encryption decrease IoT threats. The authors suggested further study to safeguard IoT devices. Lu and Xu [22] developed a taxonomy of IoT cybersecurity risks and a four-layered cybersecurity-oriented IoT architecture. They examined its applicability and attack defence methods. Harbi et al. [10] analyzed IoT security using device, transmission, and data security criteria.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 11, Issue 4, pp: (43-50), Month: October 2023 - December 2023, Available at: www.researchpublish.com

The Internet isn't just trendy; it's a necessity in today's society, evolving from a trend to a vital need. With daily advancements, leveraging the Internet for security has become indispensable for our tech-driven generation. Embracing it safeguards us in an ever-evolving technological landscape. [1]. One important applications of the Internet, among its many additional advantages, is security. The method has lessened human labour since people nowadays are less familiar with and respectful of it. One device can manage several devices, which reduces the number of people needed to manage them. [2]. Figure-1 shows the applications and formation of the IoT environment.

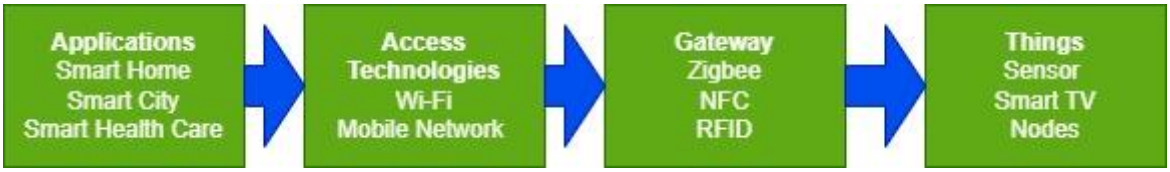

Fig. 1 Major component of IoT structure and its applications

2. RELATED WORK AND OBJECTIVES

The devices may automatically send and receive data across wireless and internet connections. Organizations and researchers define the IoT and smart surroundings. Geneiatakis et al. discussed that the IoT system gives support to various types of applications such as smart industries, smart cities, and smart homes. Smart objects used in these applications interact with other components like mobile devices, data collectors, etc. to provide various services. While providing services,it also takes users to security and privacy threats due to their limited processing. IoT in healthcare may improve patient health, engagement, and treatment. IoT devices pose substantial security, privacy, and safety threats to patients and healthcare workers. Few healthcare IoT risk reduction studies exist. Secure uses for IoT devices in healthcare have been studied. Health IoT apps are necessary since healthcare data is sensitive. Healthcare IoT appears promising. Narrowband IoT in its low-ener.gy version is popular for sensing and measurement. Energy efficiency makes it popular in healthcare. Healthcare IoT concepts exist. Unstandardized and LTE-friendly. Healthcare apps now use N.B. IoT. N.B. IoT's major dangers are security and system difficulties. It might be a feasible and popular choice for low-power, wide-area healthcare installations if these limitations are resolved. The Internet of items, which connects a wide range of items to networks to enable smart applications, must protect user privacy and prevent attacks including spoofing, DoS, jamming, and eavesdropping. The author uses supervised, unsupervised, and reinforcement learning (RL) to investigate IoT system flaws and protection strategies. Data privacy analysis examines ML-based IoT device authentication, access restriction, data offloading, and virus detection. IoT will affect society, business, and the economy. Hackers target low-resource IoT nodes. Common cryptography protocols solved IoT network security and privacy issues. IoT networks' unique characteristics and security issues cannot be solved by current solutions. ML and deep learning in devices and networks may avoid many IoT security issues. Healthcare IoT potential is intriguing. Narrowband IoT and sensing and measurement are its strengths. Healthcare uses it since it's energy efficient. IoT has several healthcare uses. LTE works well with IoT. Thus, IoT is now a feasible healthcare solution. Security and system issues are IoT's major risks. If these concerns are remedied, it might become a popular low-power, broad-area healthcare system. 2023, 13, x peer review 6 of 33 machine learning-based IoT network protection techniques. Data privacy analysis examines ML-based IoT device authentication, access restriction, data offloading, and virus detection. IoT will affect society, business, and the economy. Hackers target low-resource IoT nodes. Common cryptography protocols solved IoT network security and privacy issues. IoT networks' unique characteristics and security issues cannot be solved by current solutions. ML and deep learning in devices and networks may avoid many IoT security issues. Healthcare IoT potential is intriguing. Narrowband IoT and sensing and measurement are its strengths. Healthcare uses it since it's energy efficient. IoT has several healthcare uses. LTE works well with IoT. Thus, IoT is now a feasible healthcare solution. Security and system issues are IoT's major risks. It might become a popular low-power, broad-area healthcare system if these difficulties are remedied.

Security of IoT devices in the context of mobile computing is the security analysis of IoT using a novel approach, as indicated in Table 1 of the literature review on intelligent security by IoT.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 11, Issue 4, pp: (43-50), Month: October 2023 - December 2023, Available at: www.researchpublish.com

Table I: LITERATURE REVIEW

Ref No.	Year	Domain	Description
[11]	2017	IoT	Focuses upon requirement-based security analysis of IoT
[12]	2015	IoT	Analysed the IoT security challenges, issues and open problems
[13]	2018	IoT	Discusses the layer-based security analysis of IoT
[14]	2018	IoT	Architecture-based analysis in light of security requirements
[15]	2019	IoT	Risk assessment model for addressing the security issues in the IoT ecosystem
[16]	2018	IoT	Discusses the problem analysis of IoT layers and provide a proposed solution
[17]	2015	IoT	Discusses security aims, goals and vulnerabilities for IoT
[18]	2019	IoT	Threats and attack-based analysis of IoT computing
[19]	2016	IoT/Mobile computing	Security issues and challenges of IoT and mobile
[20]	2018	Mobile computing	Security analysis of mobile device-to-device network using the Android operating system

3. METHODOLOGY

The ability to control multiple devices from a single interface has not only improved convenience but also opened up avenues for enhancing security. For instance, smart home security systems enable remote monitoring, allowing individuals to keep an eye on their homes from anywhere in the world. IoT-enabled sensors can detect anomalies, triggering alerts in case of potential threats or hazards, thereby bolstering safety measures. IoT enables the connection of several devices so that they may all be operated or controlled by a single device [6]. Figure 2. A single device may also readily access a number of additional devices that are utilized for various reasons.

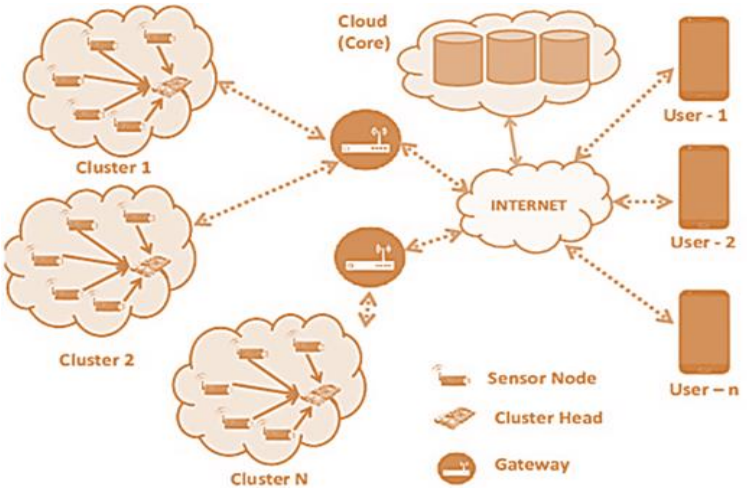

Figure 2. Different components of IoT

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 11, Issue 4, pp: (43-50), Month: October 2023 - December 2023, Available at: www.researchpublish.com

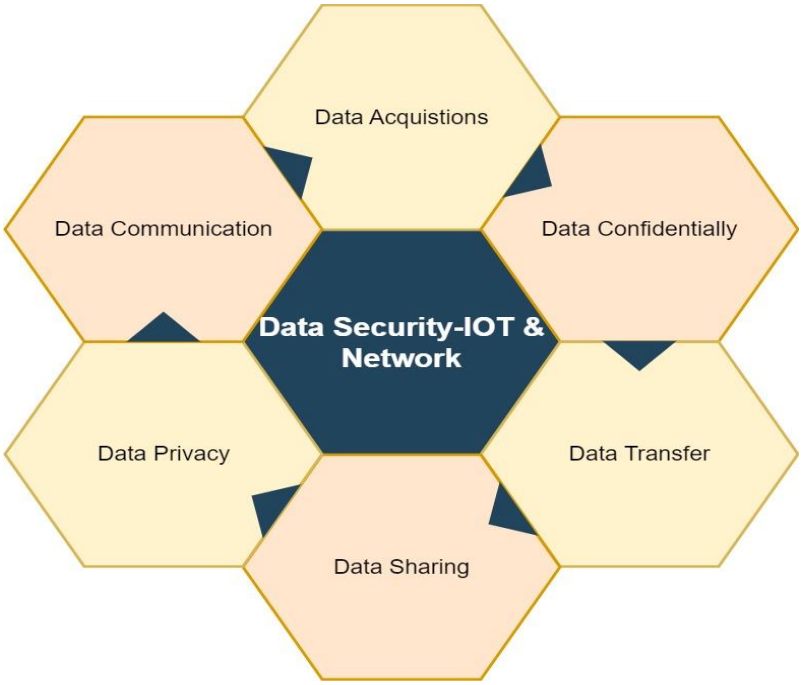

Figure 3: IoT Information Security

4. FEATURES OF SMART SECURITY

One of the main purposes of the devices included in the intelligent security system, which is currently employed for a variety of purposes, is human security. The usage of CCTV cameras and other equipment that may link to them through the internet is widespread [8]. Anywhere has access to surveillance cameras with night vision recording capabilities. As shown in table 2 [9], we have successfully dealt with numerous dangerous situations and threats to human life with the aid of the Internet.

TABLE II: FEATURES OF SMART SECURITY

Features	Effects
Accessibility	Easily accessible and saves time
Control	It can be controlled from remote locations easily
Data providing	It provides real-time data and information

A remote system called Home Automation System (H.A.S.) may also be used to operate several electrical appliances in the home [10-11]. This system's ability to save energy for those who are preoccupied or absentminded is its unjustified benefit. To ensure power efficiency, it is simple to monitor energy consumption. As a consequence, energy usage is reduced. The daily improvement of systems and equipment has defeated and surpassed the outdated approaches. This technology depends on the Internet for a number of reasons, including its many features, simplicity of access, and reduced time requirements.

Its management's connection to the Internet is the sole thing that can influence how it works [12]. An illustration of a home automation system's operation is shown below. Another great example of this type of technology that is already available on the market and that can be utilized and managed in a similar way utilizing the same internet connection are smart geysers. With just a flick of the fingertips, people may immediately access hot water. Utilizing such modernized electronic products for home needs has made it simple to conserve time and energy, as illustrated in figure 3.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 11, Issue 4, pp: (43-50), Month: October 2023 - December 2023, Available at: www.researchpublish.com

5. IMPACTS OF THE INTERNET OF THINGS ON SMART SECURITY

Without the Internet of Things, intelligent security systems would be insufficient since smart security consists of easily accessible resources that can be accessed from anywhere at any time with an internet connection and such gadgets that the Internet can access. Smart technologies and the internet system have improved and made home security safer. A new age for the current technological revolution has arrived with the introduction of innovative home alarm systems and night vision cameras for security surveillance [13]. Without incurring additional costs, millions of data may be acquired, analyzed, and kept in a lot less time. The Deep Learning technique, firstly, the architecture design of the convolutional neural Network (CNN) community is presented and analyzed within the context associated with selected and designed architecture from the surveillance system Fig.-3 shows a H.A.S. modal.

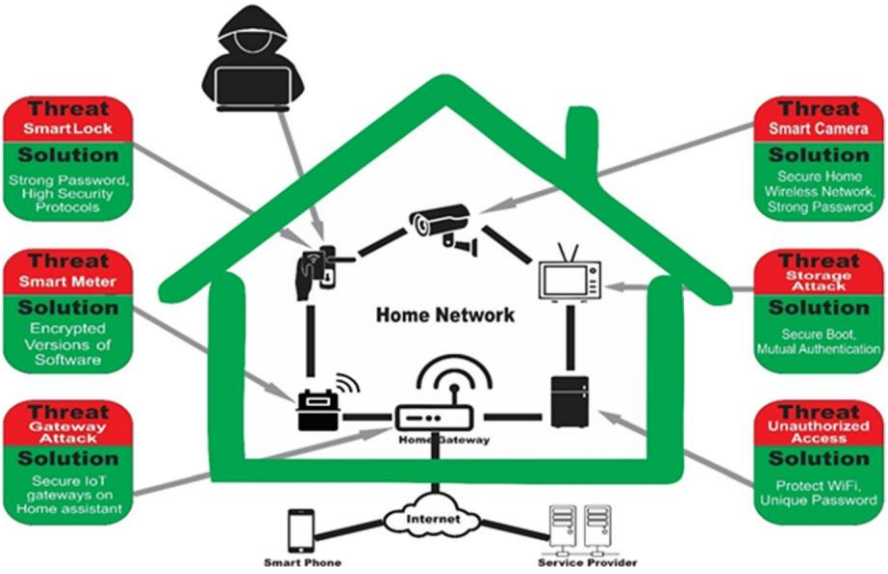

Figure 4. H.A.S. model

6. SMART SECURITY FOR WOMEN SAFETY

Many tools have been developed utilizing internet technology to prevent crimes and to identify the suspect using a variety of techniques, such as face-recognition software caught by a security camera, as illustrated in figure 4.

A.E.S.H.S.: A gadget employing GPS technology is thought to be superior for this sort of task called as Advanced Electronic System for Human Safety in order to locate an individual's position when they are in danger or stuck in a difficult scenario and to get them out of that dilemma. The ILA Security system protects the victim from perilous circumstances by having three personal alarms that can startle and confuse intruders. These were only a handful of the many different tools utilized to keep people safe. An intelligent security system called H.A.S. uses IoT technology.

- ***Smart Belt***: The apparatus has a belt-like portable gadget in its design. It includes an Arduino Board, a shrill siren, and a pressure sensor [14]. Screaming alarm system activates, sending off sirens to summon assistance. This belt also has certain disadvantages in that the victim must initiate the activity, which does not occur in these situations. Finding a remedy to this issue that operates independently in these interactions is therefore of utmost importance.

- ***Motion Sensor***: a tool that can track any moving item. The tool operates automatically and informs the user of the option in a specific location. These sensors are crucial for human security as well [15].

Numerous situations involving persons being monetarily humiliated or having personal information disclosed were recorded and registered in the thousands [16]. These people take advantage of the Internet's capabilities for personal gain and financial exploitation of others. Sometimes the effects are even worse, as seen in figure 5. To avoid falling for these sorts of scams, a person needs to be highly responsible and educated. Figure 6 illustrates how a hacker may occasionally get access to a user's social media account and endanger their data and privacy [17].

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 11, Issue 4, pp: (43-50), Month: October 2023 - December 2023, Available at: www.researchpublish.com

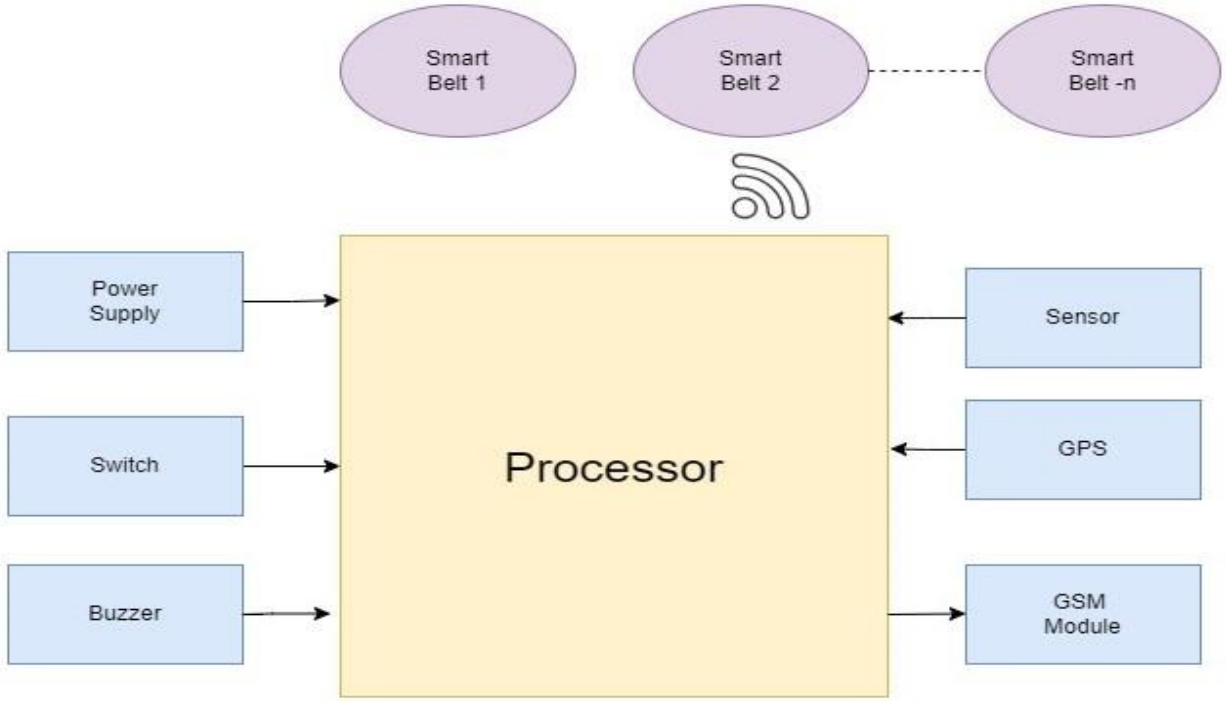

Figure 5. Blocks of Smart Belt

7. THREAT IMPLICATIONS OF IOT

There are many millions of Android phones, Smart Tablets, Laptops, and Computers available. They are widely used by consumers, who either utilize them for Internet-based work or web surfing to gather and research data and information for their needs [18]. Social media has helped a lot of individuals connect with their loved ones all around the world. By utilizing false information and bogus accounts, many fraudulent users try to trick people. Because of the photographs they use as their account images, people get duped by false accounts. Knowing the most recent technologies offers benefits and drawbacks. Similar characteristics may also be seen in the Internet of Things, but it also has significant drawbacks [19]. The first issue is that a lot of people still need to be educated on how IoT should be used. Few people are aware of its purpose, how to use it, etc. People need to be aware of and knowledgeable about how to use such cutting-edge technologies [20]. Most departments still need to be mended, but only a small number of departments in many nations can effectively exploit such apparatus to their own advantage [21].

The possibility of hacking is another drawback of this technology. Hackers are becoming more knowledgeable on how to utilize and abuse the most recent technologies as the modern world advances. It's possible for a business or organization to go bankrupt or for there to be another cyberattack. It will cause the value of that company's shares to decline and cause it to lose the credibility and confidence of its investors. If such data spills, it risked losing its position in the world market. People learn about their company's goals and marketing efforts as private and secret information is released [22].

They still don't know their secret to success, and numerous rivals might take advantage of this situation. There are some drawbacks to benefits.

The process of agriculture has evolved as a result of security using intelligent system approaches. Agriculture practices from the past could have been more advantageous than those used now, which rely on information and communication technology. By keeping an eye on them using the most recent and enhanced security systems, it is simple to monitor and safeguard the quality of grains before or after harvest. Crop loss results from the harm caused by rodents. To protect the crops from danger, it is possible to drive the rodents away from agricultural fields. This is why agriculture uses IoT-based smart security. In addition, monitoring water quality, intelligent greenhouses, and water quality may all be maintained under control [23].

8. CONCLUSION

Today, we frequently utilize the Internet for a variety of objectives in our daily lives. By offering a variety of services including access surveillance, human security against attacks, etc., smart security satisfies the demands of the modern world.

For several objectives, including gathering and processing real-time data, security warnings, and surveillance, smart security systems have become essential. In addition, it is utilized for other fundamental requirements including finding someone in an emergency and tracking whereabouts. It incorporates safeguards for everyone's safety, which are covered in more detail in this page.

REFERENCES

[1] N. N. Dlamini and K. Johnston, "The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review," in Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE), Nov. 2016, pp. 430–436.

[2] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[3] D. Eckhoff and I. Wagner, "Privacy in the smart city Applications, technologies, challenges, and solutions," IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 489–516, Sep. 2018.

[4] X. Xia, Y. Xiao, and W. Liang, "ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 445–458, Feb. 2019.

[5] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a secure wireless-based home area network for metering in smart grids," IEEE Syst. J., vol. 8, no. 2, pp. 509–520, Jun. 2014.

[6] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019.

[7] S. Kumar, S. Rani, A. Jain, C. Verma, M. S. Raboaca, Z. Illés, and B. C. Neagu, "Face spoofing, age, gender and facial expression recognition using advance neural network architecture-based biometric system," in Sensors, vol. 22, no. 14, pp. 5160, 2022.

[8] J. Jain, A. Jain, S. K. Srivastava, C. Verma, M. S. Raboaca, and Z. Illés, "Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA," in Mathematics, vol. 10, no. 7, pp. 1071, 2022.

[9] A. Jain, R. K. Dwivedi, H. Alshazly, A. Kumar, S. Bourouis, and M. Kaur, "Design and simulation of ring network-on-chip for different configured nodes," in Computers, Materials & Continua, vol. 71, no. 2, pp. 4085-4100, 2022.

[10] NFC Transponder for Enabling IoT. Accessed: Sep. 10, 2022. [Online]. Available: https://connectedworld.net/tag/transponders/

[11] N. A. Khan, M. Altaf, and F. A. Khan, "Selective encryption of JPEG images with chaotic based novel S-box," Multimedia Tools Appl., vol. 80, no. 6, pp. 9639–9656, Mar. 2021.

[12] US Food and Drug Administration. Cybersecurity Vulnerabilities Identified in St. Judge Medical's Implantable Cardiac Devices and Merlin Home Transmitter: FDA Safety Communication. Accessed: Sep. 20, 2022. [Online]. Available:https://www.dicardiology.com/article/fdaonfirmscybersecurityvulnerabilities-st-judes-implantable-cardiac-devices-merlin

[13] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and G. Saldamli, "Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model," in Proc. 4th Int. Conf. Multimedia Comput., Netw. Appl. (MCNA), Oct. 2020, pp. 113–118, doi: 10.1109/mcna50957.2020.9264301.

[14] V. Cortier, P. Gaudry, and S. Glondu, "Belenios: A simple private and verifiable electronic voting system," in Foundations of Security, Protocols, and Equational Reasoning. Cham, Switzerland: Springer, 2019, pp. 214–238.

[15] S. Kremer and P. B. Ronne, ‘‘To du or not to du: A security analysis of du: A security analysis of du-vote,’’ in Proc. IEEE Eur. Symp. Secur. Privacy, Mar. 2016, pp. 473–486.

[16] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, ‘‘State-of-the-art survey of artificial intelligent techniques for IoT security,’’ Comput. Netw., vol. 206, pp. 1–56, 2022, doi: 10.1016/j.comnet.2022.108771.

[17] UK Government Developer Documents. Accessed: Jun. 12, 2022. [Online]. Available: https://assets.publishing.service.gov.uk/

[18] M. Ehret and J. Wirtz, ‘‘Unlocking value from machines: Business models and the industrial Internet of Things,’’ J. Marketing Manage., vol. 33, nos. 1–2, pp. 111–130, Jan. 2017.

[19] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, ‘‘A risk assessment methodology for the Internet of Things,’’ Comput. Commun., vol. 129, pp. 67–79, Sep. 2018.

[20] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-porisini, ‘‘REATO: REActing to denial of service attacks in the Internet of Things,’’ Comput. Netw., vol. 137, pp. 37–48, Jun. 2018.

[21] G. Yang, ‘‘An overview of current solutions for privacy in the Internet of Things,’’ Frontiers Artif. Intell., vol. 5, pp. 1–8, Mar. 2022.

[22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, ‘‘A survey on security and privacy issues in Internet-of-Things,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[23] A. Mosenia and N. K. Jha, ‘‘A comprehensive study of security of Internet-of-Things,’’ IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586–602, Dec. 2016.

[24] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Zahidul H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, and J. Lindqvist, ‘‘Robustness, security and privacy in location-based services for future IoT: A survey,’’ IEEE Access, vol. 5, pp. 8956–8977, 2017.

[25] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, ‘‘IoT Middleware: A survey on issues and enabling technologies,’’ IEEE Internet Things J., vol. 4, no. 1, pp. 1–20, Feb. 2016.

[26] U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, ‘‘Trust management techniques for the Internet of Things: A survey,’’ IEEE Access, vol. 7, pp. 29763–29787, 2018.

[27] Farris, T. Taleb, Y. Khettab, and J. Song, ‘‘A survey on emerging SDN and NFV security mechanisms for IoT systems,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 812–837, 1st Quart., 2018.

[28] D. D. López, M. B. Uribe, C. S. Cely, A. V. Torres, N. M. Guataquira, S. M. Castro, P. Nespoli, and F. G. Mármol, ‘‘Shielding IoT against cyber-attacks: An event-based approach using SIEM,’’ Wireless Commun. Mobile Comput., vol. 2018, pp. 1–19, Oct. 2018.

[29] M. M. Hossain, M. Fotouhi, and R. Hasan, ‘‘Towards an analysis of security issues, challenges, and open problems in the Internet of Things,’’ in Proc. IEEE World Congr. Services, Jun. 2015, pp. 21–28.

[30] R. Román-Castro, J. López, and S. Gritzalis, ‘‘Evolution and trends in IoT security,’’ Computer, vol. 51, no. 7, pp. 16–25, 2018.

[31] Andrea, C. Chrysostomou, and G. Hadjichristofi, ‘‘Internet of Things: Security vulnerabilities and challenges,’’ in Proc. IEEE Symp. Comput. Commun. (ISCC), Jul. 2015, pp. 180–187.

[32] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, ‘‘IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201, Oct. 2019.