Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider

Eshtiak Ahmed*‡, Ashraful Islam†‡, Mohsena Ashraf§, Atiqul Islam Chowdhury¶, Mohammad Masudur Rahman||
*Tampere University, Tampere, Finland
eshtiak.ahmed@tuni.fi
†University of Louisiana at Lafayette, Louisiana, USA
ashraful.islam1@louisiana.edu
‡Daffodil International University, Dhaka, Bangladesh
{eshtiak, ashraful}.cse@diu.edu.bd
§Ahsanullah University of Science and Technology, Dhaka, Bangladesh
mohsena_ria.cse@aust.edu
¶United International University, Dhaka, Bangladesh
achowdhury201036@mscse.uiu.ac.bd
||Bangladesh University of Engineering and Technology, Dhaka, Bangladesh
masudurism@gmail.com

***Abstract*—In recent years, Internet of Things (IoT) is rapidly gaining popularity as it has a vast potential. But without proper security and privacy measures, IoT can facilitate cyberattacks as it possesses some serious issues that need to be tackled well to utilize its fullest potential. In this study, an attempt to briefly discuss the basic concept and the pros and cons of IoT was taken by the authors. Moreover, this research also highlights the basic architectural issues, vulnerabilities, and future security concerns of IoT as IoT has a cost when it comes to the case of security and privacy. In addition to that, major threats and attacks of IoT e.g. Denial of Service (DoS), Man in The Middle (MiTM), Supervisory Control and Data Acquisition (SCADA) attack were explained in brief. At last, probable measures that can be employed in order to strengthen the security of IoT were underlined so that the advantages of IoT can be reaped mostly in terms of security and privacy.**

***Index Terms*—Internet of Things, IoT, Security and privacy, DoS attack, IoT framework**

I. Introduction

Recent advancements in modern technology have prioritized internet-enabled devices above all as they provide significantly more value compared to previously available devices. Almost all the consumer devices have been given internet access capabilities in order to enable smart functionalities. These internet-enabled devices or things that are capable to connect with each other through the internet are referred to as Internet of Things (IoT) [1] [2]. Its also dubbed as the Future Internet [3]. IoT is a technology that refers to technologically enables objects being part of the internet; each of these objects is uniquely identified, and accessible through a network infrastructure, performing real-time perception, data analysis and providing assistance to the people using it [4].

According to Statista, 23.14 billion IoT devices are installed within 2018 while this number is expected to grow to an astonishing 42.62 billion by the year 2022 [5]. They have also predicted that this number will grow in leaps and bounds and there will be nearly 75 billion IoT devices within 2025. Every other devices in our daily lives such as TVs, fridges, alarm systems, smoke detectors, and vehicles are being given the access to the internet, thus adding to the internet of things. From the start of the advancement in IoT, it has been adopted to many sectors of technology and created a revolution all through. It has become hard to find a home that does not have at least a single IoT enabled device [6].

IoT has become such a significant technology in recent times, not just because of its usefulness, but also because of the seamless integration with our day to day lives. However, the advantages are not all there is as it comes with plenty of vulnerabilities [2] [7]. In this study, along with the pros and cons of IoT technology, vulnerability issues and security concerns are discussed in terms of real life usage and technical aspects.

Remaining part of this article is structured as follows: In Section II, advantages and shortcomings of IoT are presented. In Section III, vulnerabilities issues of IoT are discussed. Section IV discusses the future prospects and security concerns of IoT based on real life events. Section V reflects on possible measures to be taken in order to minimize IoT vulnerabilities. Finally Section VI concludes the article.

II. IoT Advantages and Shortcomings

A major reason behind this acceptability of IoT leads back to the advantages and convenience that IoT has provided. In the following sections, both the advantages and shortcomings of IoT are discussed.

A. Advantages of IoT

1) Ease of Accessing Information: IoT technology allows to access data and information easily from anywhere in the world given the proper internet connection, that too in real time. This is made possible by the interconnected network of sharing enabled devices. Physical presence has become somewhat unimportant when it comes to get work done, adding a much needed convenience to what people do.

2) Communication: IoT has taken the communication sector by storm by creating the possibility to have a network of interconnected devices. Communication devices are made more transparent, reducing inefficiencies in communication. Its not just human to human or human to machine communication that has got an upgrade, but machine to machine communication has been made possible and more efficient through IoT, producing faster results.

3) Automation and Control: IoT has allowed physical objects and machines to be connected and enabled to be controlled digitally and virtually with the help of wireless infrastructure, automation has become a common thing [8]. These devices can be controlled from miles apart and need no physical intervention from human beings. This also allows machines to communicate with each other according to pre-set protocols, making the process much more efficient.

4) Cost-effectiveness: Arguably the biggest advantage of IoT is how it benefits us financially. Physical interventions have been minimized, as a result movement and logistics costs have been minimized. It also appears to be helpful for people in daily lives as they can communicate with either other people or home appliances easily, saving valuable energy as well as money in the process.

5) Monitoring: Being able to monitor anything on real time is a massive advantage of IoT. Monitoring is not limited to industrial aspects, nowadays home monitoring has been more of a common norm, thanks to IoT advancements. People can monitor their house condition, temperature inside and many more. In addition to monitoring, IoT allows to control all aspects inside a home remotely such as controlling the temperature, opening or closing windows etc. [8].

Health monitoring is another sector IoT has added benefits to. There are devices available which monitor health conditions of human body on the go like heart rate, pulse and blood pressure. Real time monitoring of these vital aspects of human health can lead to important health discoveries [9] [10]. These devices can track changes in heart rate and blood pressure and detect any abnormalities in them. In times of emergencies, these devices are able to contact responsible person and literally save lives, making the user more independent and risk free.

B. Shortcomings of IoT

There are numerous advantages of IoT, but its not all positive all the way. There are several disadvantages which are discussed in the following section.

1) Compatibility Issues: A big number of IoT enabled devices have been introduced in the recent times and more are on the way. But, they do not have a common technology or framework. This creates a compatibility issue in making them collaborate. As network technologies there are several that are used like Bluetooth, Wi-Fi and usb. Because of different technologies and their different working principles, their compatibility factors take a hit. A proper streamlined framework could solve this problem.

2) Employability Issues: Its always the bitter truth that, with the advancement of technology, certain types of jobs are going to get extinct. Machines and devices will replace some human jobs. On the other hand, more jobs will be created, however these will need more technical competence.

3) Privacy and Security Issues: Privacy and security is by far the biggest issue of the advancement of IoT [11]. There are a lot of connected devices that are transmitting big chunks of data every second. Majority of this data contain personal information like personal conversation, home environment settings, health tracking data and so on. What if these data get stolen and fall in wrong hands?

It could prove to be a disaster if personal information goes public. Worse would be if intruders are able to manipulate that data. They can change the temperature, send malicious messages to related ones and so on. This is the issue that is needed to be taken care the most.

III. IoT Vulnerabilities

While the number of IoT devices are increasing day by day, the security aspect of it is becoming exponentially challenging. Increased number of devices mean increased security threats, more vulnerabilities, and more users personal data and identity being compromised [12].

A. Architectural Issues

The basic architecture of IoT includes 3 major layers- perception layer, network layer and application layer [3] [4]. Although there are a number of different layered architectures of IoT [5] [13], those are created based on the common three layer architectures by improving or modifying different aspects, shown in the Fig. 1. Roles and security issues in the core layers are discussed individually below:

1) Perception Layer: This layer is used to sense the environment and surroundings to collect information that will be used to take decisions/actuations later on. The main component of this layer is sensors. They sense the environment and collect information, then transfers in to the application layer via the network layer. The major security issues of this layer are node authentication and lack of data encryption after sensing, authentication and confidentiality [12].

2) Network Layer: This layer has the responsibility to make transmissions reliable which can include information and data communications. The common security threats of this layer is DDoS attacks, Man-in-the-middle attacks and data confidentiality [14]. The most vulnerable component of this layer is the routing of data and information. As a result, attacks while routing is one of the most common issue for this layer which usually takes place while forwarding data from one layer to another.

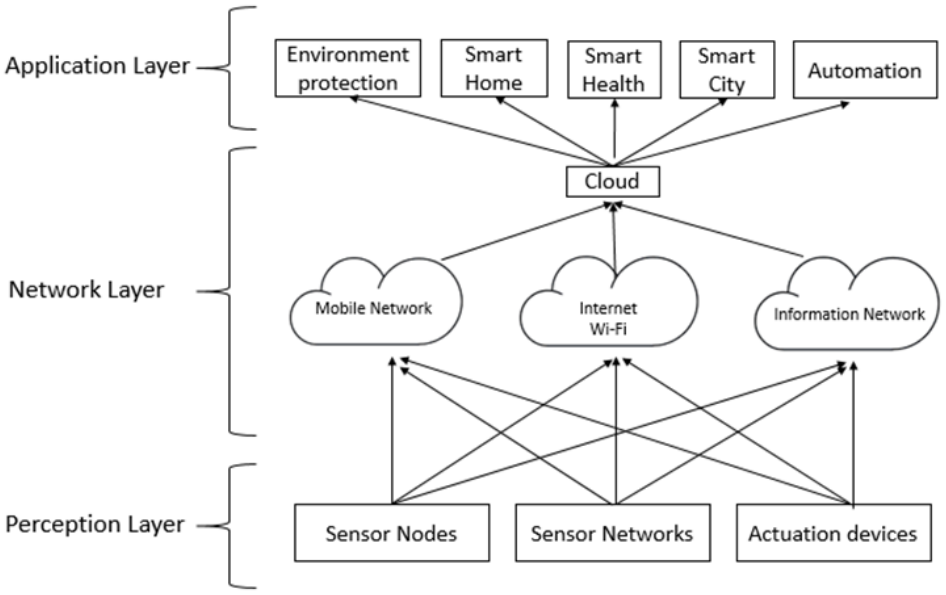

Fig. 1. Basic three layers of IoT architecture

3) Application Layer: The application layer is responsible establishing a connection between the devices and the users. It takes information from the perception layer and then uses it to provide user specific actuation. Common issues if this layer are data privacy, access control and information disclosure [15] [16]. Another issue of the application layer is the insecure and weak interface of IoT devices.

B. Different Types of Vulnerabilities

While the core IoT layers are the root of the problems, vulnerabilities are not always related to the basic layers. There are so many other aspects that come into play while thinking about IoT vulnerabilities. The Open Web Application Security Project (OWASP) has identified top ten vulnerabilities of IoT [17] with systematic research and surveys. They are discussed in the following section.

1) Insecure Web Interface: Every user of a web system might not be technically sound, thus they need a graphical user interface for them to easily control and also modify the commands according to their liking. Smart devices nowadays are used by all which creates a need for simplistic interfaces. As a result, almost all smart devices have them including all the IoT devices. However, the security of web interfaces have always been a matter of concern as it's still a struggle for the software industry to ensure security of web interfaces. This can lead to a complete takeover of vulnerable devices through corruption and denial of access. In the bigger picture, these issues can compromise devices which then compromise the security of the customers.

2) Insufficient Authentication/Authorization: All smart/IoT devices have the functionality of authentication in order to ensure authorized access. But these devices along with the users are being compromised because of poor or insufficient authentication credentials. People are prone to using passwords that can be easily guessed, such as 123456, qwerty, password etc. [16] [18]. Intruders can easily hack into their systems and all their data are exposed. This might compromise the device as well as the user accounts, resulting in denial of further access. Considering a business perspective, users and accounts can be compromised along with their data being stolen and further used in forgery.

3) Insecure Network Services: Nowadays firewalls are used in almost all the enterprise solutions as part of security measures. But these measures are not well thought of while designing IoT devices. As a result, these devices are more vulnerable than other smart systems. The results of this issues can be data loss or data corruption and denial of service, leading to other connected devices to be compromised. One compromised device can make all other connected devices to become vulnerable.

4) Lack of Transport Encryption/Integrity Verification: Data collected via different types of sensors are transmitted to central server for proper actuation and manipulation of devices. But most of the time, these data are sent without any encryption and as plain readable data files [15]. As a result, if an intruder can somehow access the transmitted data, they can easily manipulate it as they are not encrypted. The result of this concern could be data loss, unauthorized data manipulation and modification. Modification of user data can lead to unexpected actuation and improper service.

5) Privacy Concerns: Sometimes IoT devices tend to demand or require data that are not necessarily mandatory in order to make the device workable. Also most of the data are stored without any encryption. This way, identity and data theft are increasing day by day. This can lead to compromise of users personal data which can cause personal attacks on users.

6) Insecure Cloud Interface: Cloud is considered to be one of the best technologies that assist IoT data management because of its availability and easier accessibility. However, this much data trafficking can lead to devastating consequences if they are not well secured. It can compromise user data and also lead to loss of control over devices. Losing control over devices can eventually lead to losing control of the whole network of IoT.

7) Insecure Mobile Interface: Almost all of the IoT devices are controlled by mobile devices or smartphones. This is a single most vulnerable weak point of IoT as it has all the access granted to the devices. If an intruder can access the mobile controller device, he can take over the whole network of things. Insecure mobile interfaces can lead to compromise and modification of users data and can also be used for forgery.

8) Insufficient Security Configurability: While proper measures are needed to be taken in order to make IoT device more secured in terms of firewall and extra layers of encryptions, further configurability is very limited. This makes the system more error prone after a while when new security threats emerge and the system needs to be updated accordingly.

9) Insecure Software/Firmware: Every IoT device runs on a specific software or firmware in order to provide better accessibility to the user. These are prone to get exposed if the underlying programs are not made well secured. Also, these firmware need to be updated time to time to keep them secure from new security threats.

10) Poor Physical Security: Physical accessibility of a device can be very crucial as it ownership can change depending on them. If a device is shared by multiple users, being vulnerable can cause a lot more damage that if used personally. While shared usage is considered to be a feature, it can make the whole user base vulnerable. These aspects need to be taken into account.

IV. Future Prospects and Security Concerns in IoT

While the number of IoT devices are increasing day by day, the security aspect of it is becoming more and more challenging. More devices mean more security threats, more vulnerabilities and more users personal data and identity being compromised [16].

Attacks on internet connected devices are not a new phenomenon. However, the newest concern is the security of IoT devices as they have minor to no security while being developed on a large scale. Every other device in our daily lives such as TVs, fridges, alarm systems, smoke detectors, vehicles are being given the access to internet, thus adding to the internet of things. While being useful, these devices are adding to the existing vulnerable devices, if proper measures are not taken. Major threats and attacks that are existing in IoT are discussed in the following section.

A. Denial of Service (DoS) Attack

A denial of service (DoS) [19] attack refers to unavailability of service or infrastructure due to capacity overload. In comparison to other types of attacks, the nature of DoS is a bit different. It does not concern with stealing information or loss of security, but affects services in terms of reputation and availability which can cause loss of good will and also financial strength. A popular form of DoS is Distributed Denial of Service (DDoS) attack in which a large number of systems maliciously attack one target or service.

The Mirai DDoS attacks [19] on the Dyn network were the biggest ever in history, having reported an attack which had a strength of 1.2 Tbps, taking down more than 80 major websites including Netflix, Twitter, Reddit, the Guardian and CNN. This was caused by a IoT botnet which was created by malware named Mirai. Once infected with Mirai, devices continuously keeps searching the internet for vulnerable IoT devices, then use known default usernames and passwords to login, infecting them with malware. Another major example is BBC domain attack in 2016. In 2016, a DDoS attack was launched on the BBC's website taking down the entire domain which then included their on-demand television and radio player, keeping them out of service for more than three hours. In November 2016, at least 5 Russian banks were hit by a DDoS attack that kept their service down for nearly 2 days.

These kind of attacks are usually performed using a botnet, a lot of devices are programmed and controlled in such a way that they all will send connection request to a service at a specific time-frame, all of these being unknown to the owner. As the number of IoT devices that are connected together is in the millions, if they are compromised, huge waves of DDoS attacks can be generated by them. Insecure web interface, insufficient authentication and security configurability and out of date security firmware are the main reasons of this kind of vulnerabilities.

B. Man in The Middle (MiTM) Attack

The concept of man-in-the-middle is while an intruder or attacker tries to get into communication streams between multiple users or systems. It's possible for such attackers to intercept and change messaged of either or both end without them having any idea that someone is listening to them. As the original communication flows through the attacker, they can easily make the recipient believe that they are still receiving a message from the actual recipient. Attacks on home routers can collect personal data and user credentials for online accounts and corporate networks.

For this type of attacks to happen, attackers usually target the TCP connection established between server and client in any http communication. The attacker can use multiple techniques, splitting the actual TCP connection, creating 2 different connections, one connecting the attacker and the client and the other connects the server and the attacker. As soon as the TCP connection is split, the interceptor can start acting as a proxy server. This allows the attacker to read and modify the data, while inserting is another possibility. Insecure network services and lack of transport encryption are the causes of this kind of attacks in IoT.

C. Supervisory Control and Data Acquisition (SCADA) Attack

These kinds of attacks are made on machines or devices that communicate to convey feedback between systems [20] [21]. Attacker tries to take control of the device and can manipulate feedbacks including actuation commands for the end users. These can lead to disasters especially for smart home appliances.

In early 2017, St. Jude Medical in USA reported that their implantable cardiac devices had security issues that could potentially allow an intruder to gain access of the device [22]. This vulnerability concerned the transmitter of the device that works to take and share data to the physicians remotely [23]. It was evident that this device could be controlled if someone can access the transmitter.

D. Data and Identity Theft

The main strategy for performing identity theft is to amass data. In this era of socialization, there are numerous sources of data which can provide a fully fledged overview of a user. The sources can be social media information, data from IoT devices such as smart watches or fitness trackers etc [20]. Having access to more data makes a user makes more vulnerable to attacks and they are prone to being targets more often than not.

While the IoT devices are very useful, they collect a lot of data that, if goes into wrong hands can cause disasters. There needs to be a proper protocol for these devices about the type of data they collect and the data they transmit to the cloud servers. Lack of protocol and proper standardization leads to data leak and huge amount unorganized data can be manipulated to use against the users.

E. Issues in IoT Framework

The framework of IoT has been developed and enhanced significantly over the years. In spite of these developments, the current frameworks still have security loopholes because of which the attacks have not stopped from happening. Fig. 2 shows the basic framework of IoT. Recent attacks suggest that there are several vulnerabilities in this framework. Attackers can access IoT hardware as a result of low security configurability, insufficient authentication schemes and poor backend structure. DDoS attacks, identity theft, data theft, wrong actuation happen because of this issue [24]. The communication between hardware and cloud servers is another portion that is very much vulnerable. Transmission protocols are prone to hacking and also there is little to none data encryption. As a result, Man in the Middle attacks happen, thus data manipulation and tampering takes place.

V. Possible Measures to be Taken

As the number of IoT devices are growing day by day, more people are being exposed to dangers through them [25]. However, Security has to be ensured while a system is at design and execution phase and IoT needs to be made more secure with a widely accepted and robust structure [26]. The major types of attacks are discussed in the previous section which also needs to be addressed while trying to secure IoT.

From the analysis of IoT vulnerabilities and the types frameworks is used nowadays, it can be concluded that enhancing the current architecture of IoT as well as a more effective frameworks for designing and developing IoT networks can be a viable solution to the current vulnerability issues. The following aspects need to be addressed:

- Enhancement of currently available multi-layer IoT architecture keeping the focus on interfaces, transmission security, physical security and data encryption methods.
- IoT security algorithms need to be redesigned and improved for making them more robust and less error prone.
- A proper common standard for developing IoT platforms need to be developed as there are currently no common standard in the market.

The main focus should be modifying the states of interconnected devices that ensures intelligence, ensuring security of information for its users, building trust and privacy [6]. Many frameworks have been developed to make IoT more secure, yet there are still so many vulnerabilities. A new framework needs to be designed which will be more widely expected. Following is a more detailed outline of methodologies that can be employed.

- Specific vulnerabilities need to be identified along with their root cause analysis to find out how they make the IoT devices vulnerable and what measures need to be employed in order to eradicate them.
- All the data manipulation, transmission and actuation protocols of IoT need to be studied to find protocol limitations and suggest improvements if necessary.
- All the algorithms associated with IoT need to be checked thoroughly to find out loopholes or limitations that could cause data leakage or theft.
- Cutting edge security technologies such as Blockchain [27] [28] technology can be studied and assessed to find out if they can be employed with current IoT frameworks to make them more secure in terms of data transmission and authenticity of data [29] [30].
- Any new framework will need to be implemented and

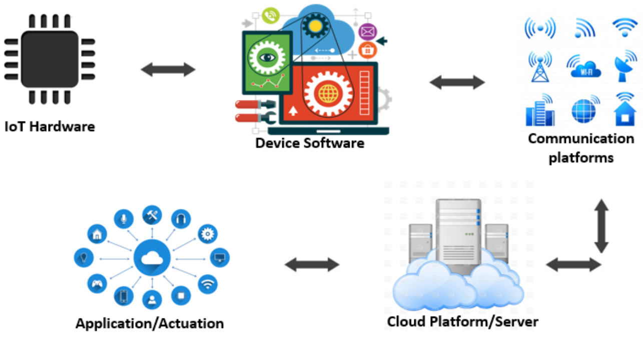

Fig. 2. Basic IoT Framework

tested with real time systems to ensure its effectiveness.

VI. Conclusions

The IoT technology has been emerging very rapidly in recent times. However, its being held down by the increasing security concerns which can be categorized into privacy concerns and unauthorized access to personal information in general. In this article, the concept of IoT has been discussed from different aspects such as pros, cons, concerns and vulnerabilities. The advantages of IoT, such as automation and control, cost-effectiveness, etc were briefly explained followed by its shortcomings regarding compatibility, employability, privacy, and security issues. Moreover, the vulnerability issues of IoT were delineated along with its basic architecture. Roles and security issues at each layer in the IoT protocol stack, i.e. perception layer, network layer, and application layer, were described concisely followed by a brief review of IoT vulnerabilities such as insecure web interface, insufficient authorization, privacy concerns, poor physical security, etc. Major threats and attacks like Denial of Service (DoS) attack, Man in the Middle (MiTM) attack, Supervisory and Data Acquisition (SCADA) attack, data and identity theft were highlighted as well.

In addition to describing all possible vulnerabilities and security concerns if IoT, the paper also suggested some measures that need to be taken in terms of security and privacy. However, at this point of time, the recommendations and suggestions are made on a very high level context and considers the theoretical aspects only. This study does not concern with any type of practical implementations thus far which could be interpreted as a limitation of this work. These possible solutions need to be implemented implemented, integrated and tested to greater extents in order to understand their viability.

References

[1] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "Iot connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67 646–67 673, 2020.

[2] A. Kim, J. Oh, J. Ryu, and K. Lee, "A review of insider threat detection approaches with iot perspective," *IEEE Access*, vol. 8, pp. 78 847–78 867, 2020.

[3] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 5. IEEE, 2010, pp. V5–484.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[5] Statista, *Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (In Billions)*. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connecteddevices-worldwide/

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[7] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an internet of secure things: A survey on issues and enabling technologies," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1372–1391, 2020.

[8] E. Ahmed, A. Islam, F. Sarker, M. N. Huda, and K. Abdullah-Al-Mamun, "A road to independent living with smart homes for people with disabilities," in *2016 5th International Conference on Informatics, Electronics and Vision (ICIEV)*. IEEE, 2016, pp. 472–477.

[9] F. Wu, T. Wu, and M. R. Yuce, "An internet-of-things (iot) network system for connected safety and health monitoring applications," *Sensors*, vol. 19, no. 1, p. 21, 2019.

[10] L. M. Dang, M. Piran, D. Han, K. Min, H. Moon *et al.*, "A survey on internet of things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, p. 768, 2019.

[11] D. Singh, B. Pati, C. R. Panigrahi, and S. Swagatika, "Security issues in iot and their countermeasures in smart city applications," in *Advanced Computing and Intelligent Engineering*. Springer, 2020, pp. 301–313.

[12] K. Laeeq and J. A. Shamsi, "A study of security issues, vulnerabilities and challenges in internet of things," *Securing Cyber-Physical Systems*, vol. 10, 2015.

[13] A. Tewari and B. Gupta, "Security, privacy and trust of different layers in internet-of-things (iots) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, 2020.

[14] J. Qian, H. Xu, and P. Li, "A novel secure architecture for the internet of things," in *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*. IEEE, 2016, pp. 398–401.

[15] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, vol. 3. IEEE, 2012, pp. 648–651.

[16] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the internet of things (iot): A comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.

[17] OWASP, *Top Ten Vulnerabilities of IoT*. [Online]. Available: https://www.owasp.org/index.php/TopIoTVulnerabilities

[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[19] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, pp. 80–84, 01 2017.

[20] M. Abomhara, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[21] Y. Lu and L. Da Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2018.

[22] F. Restuccia, S. DOro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[23] F. Popentiu-Vladicescu, G. Albeanu, and H. Madesn, "Reliability of modern engineering systems-towards a safer world," in *2nd International Conference on Computing, Mathematics and Engineering Technologies 2019*. IEEE, 2019.

[24] S. Jeong, W. Na, J. Kim, and S. Cho, "Internet of things for smart manufacturing system: Trust issues in resource allocation," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4418–4427, 2018.

[25] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for iot-based smart homes," *Sensors*, vol. 18, p. 817, 03 2018.

[26] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[27] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/

[28] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[29] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[30] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale internet of things data storage and protection," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 762–771, 2018.