EAI Endorsed Transactions
on Cloud Systems
Research Article EAI.EU

Investigating the IoT Security and Privacy Challenges: Summary and Recommendations

Premlata Chauhan[1], Shafeeq Ahmad[1], Pervez Rauf Khan[1] and Naseem Ahmad Khan[1,*]

[1]Department of Computer Science & Engineering, Azad Institute of Engineering & Technology, Lucknow, Uttar Pradesh, India

Abstract

With the development of innovative technology transformation like cloud and Internet of Things (IoT), more technology companies are pursuing research in employing such innovations. Smart homes and cities are just two examples of the many systems and technologies that the IoT can endorse. IoT - based smart objects communicate with other parts, such as proxies, portable devices, as well as data collectors. Although these components help to tackle a number of societal issues and offer users new, cutting-edge services, their confined processing power makes them susceptible to well-known privacy and security attacks. This in turn highlights the demand for a strong technical as well as legislative foundation and asserts the significance of validity and reliability in IoT. This paper provides an insight of the IoT, security, as well as privacy challenges, and also discusses the recommendations for IoT solutions. Further we also highlighting some unresolved problems that require further study.

Keywords: Internet of Things, IoT Systems, security, privacy, cyber-attack

Received on 21 July 2022, accepted on 24 August 2022, published on 31 August 2022

doi: 10.4108/eetcs.v7i22.2652

*Corresponding author. Email: naseemkhan033@gmail.com

1. Introduction

The term "Internet of Things" (IoT) refers to a broad perspective, but it can be summed up as an environment of intelligent objects equipped with networks, sensors, as well as processing tools. It combines and operates as a unit to build a setting where end users can access intelligent services. IoT is a new technology system that provides the various objects in our environment to connect with one another via sensors and the internet to improve our quality of life. The next stage of the digital revolution is known as the Internet of Things (IoT). Physical objects can now be used in digital spaces thanks to technology. Many people don't understand technology, despite the IoT's growing popularity [1–5].

There are numerous industries where this new class of IoT cloud services is present. IoT systems presently span a variety of challenging industries, including production as well as the automotive sector, farming, the healthcare system, building automation, security, and rescue services, amongst many others. IoT makes it possible to create and use smart devices to address problems and challenges in the actual world. Because of this, the majority of us are characterised by numerous "smart devices" such as home automation, smart appliances, smart televisions, wearable technology, etc. that certainly assist us live simpler, more streamlined lifestyles. The Smart Health Sensing system (SHSS) is just one instance of an IoT success. It is a small, automatic machine that keeps an eye on our wellbeing. To keep an eye on patients' crucial medical problems, this device is primarily utilised in the healthcare industry in health facilities, particularly in trauma centres. There is no question that the introduction of the internet as well as connected gadgets into our daily lives has had a beneficial result [6–10]. Figure 1 shows the size of the IoT security market worldwide form 2016 to 2025.

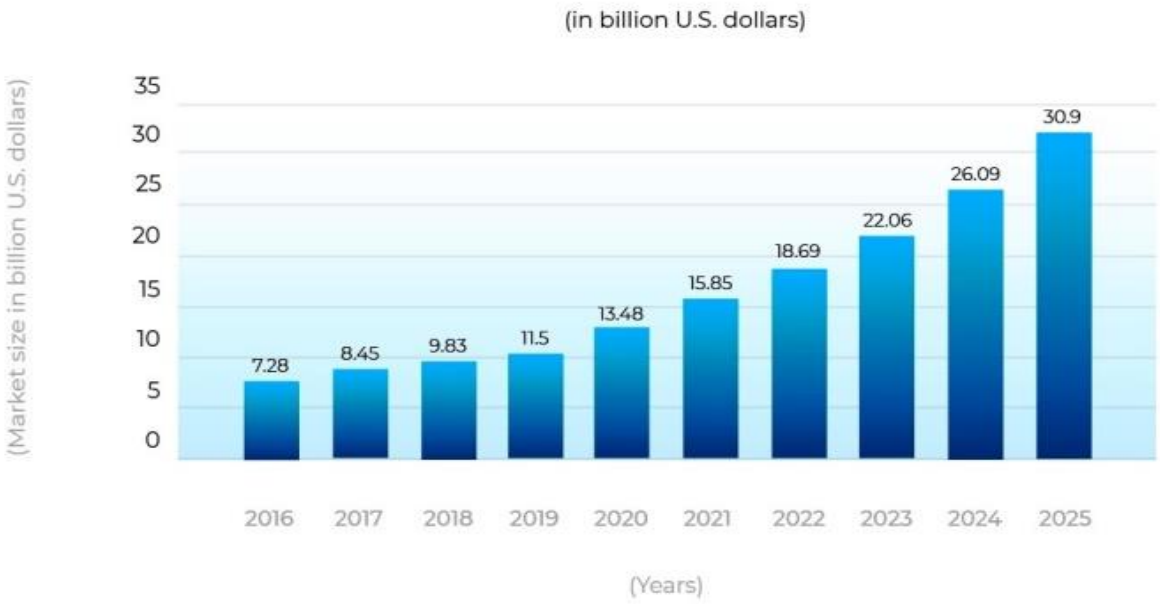

Figure 1. Size of the Internet of Things (IoT) security market worldwide form 2016 to 2025 (Source: Statista.com)

Many businesses are implementing IoT to obtain a marketable advantage. They are concentrating on improving operations and maintenance efficiency by process automation as well as real-time information management. This gives them the freedom to encounter business expansion and development in a more creative manner. Organizations are now able to design as well as implement more appropriate management strategies due to recent IoT applications. Businesses are benefiting from technology through increased operational efficiency. Advanced features like workflow automation as well as device wireless system are supported by IoT gadgets. Companies are capable of maintaining an ideal balance among energy use and sustainability as a consequence. Businesses can lessen their carbon ecological footprint by being much more energy-efficient [11–13].

The Internet of Things (IoT) has evolved over the last ten years from a fledgling technology that few individuals normally took it seriously to a true digital technology mechanism that is transforming businesses all over industry sectors as well as continents. IoT network security worries are becoming more common as more businesses incorporate IoT equipment into their services and infrastructure. Increased usability and performance emerge with a challenge called network vulnerability. The more interconnected devices user have in their ecosystem, the much more prospective entry points there are for cybercriminals to compromise your system and carry out their evil intentions. Understanding the primary threats to IoT advancement is essential as the Internet of Things grows and becomes more prevalent every year. Users might be focused on finding and strengthening their IoT digital environment if user intend to or have already adopted this new technology in their business [14–16].

Data security concerns attributed to the shortage of trained manpower are cited by 32% of organisations who have already implemented IoT as their primary priority for their IoT environment worldwide. Cyberattack on gadgets are the top concern, according to 33% of such organisations. Despite all the positive effects of IoT as well as the possible economic rewards it offers, the system is vulnerable due to the sheer volume of connected devices that are in the hands of various users in various locations. The staff's shortage of security understanding is a serious problem, and some of their staff members may not complain to secure the whole of their network devices appropriately. Up to 40 billion smart devices would therefore exist on the globe by 2025, as well as the amount of these devices would then increase within the company as well. This implies that individuals must make as soon as possible investments in the security of thier IoT ecosystem. The business becomes more susceptible as user adds more devices because it becomes approximately difficult to sustain all of the interactions among the employees' connected machines. Promoting employee security understanding as well as enhancing the security of the boundary entities are the reasonable alternatives in this situation. In simple terms, everything comes down to providing your staff with instruction on how to utilise the equipment safely and securely as well as putting in place the necessary security safeguards, including identity verification processes, physical device safeguards, anomalous identification, encrypted information exchanges, network-based firewalls, and much more [17–20].

Cybercriminals have an increasing variety of ways to violate ones security, gain access to sensitive information, as well as even steal thier assets due to the ever-increasing volume of data as well as the number of components. This

shouldn't be permitted, and despite the importance of trustworthy security measures, all of the attempts might fail simply because the staff isn't being careful sufficiently. Because of this, users should concentrate on creating a corporate culture where employees take the security of company assets very seriously. The IoT security industry is expected to increase in size from 15.8 billion in 2021 to 18.6 billion in 2022. Everything is related to the rise in connected gadgets, which unquestionably require serious security. Such IoT handset security facts and figures are not at all shocking, as security firmware would become more crucial than ever in the upcoming ten years.

The remainder of this article is organized as follows: Section 2 presents the review of different available literatures in this domain. This is followed by a thorough IoT security and privacy challenges analysis in Section 3. In Section 4, we present the security and privacy taxonomy of IoT systems and in Section 5, we enumerate our recommendations for IoT security and privacy issues outlined in the previous sections. Finally, we will conclude this article in Section 6.

2. Related Works

Iqbal et al. [21] provided a summary of IoT security and privacy obstacles, current security alternatives, as well as some research directions questions. By conducting a thorough literature review, Liao et al. [22] outlined the security issues and challenges that IoT devices face. After which, through offering potential security interventions and solutions, portable computing was used to fix these difficulties. Mobile computing has developed solutions for the IoT security issues that are premised on hardware as well as software. According to them their work was the first attempt to analyse the security concerns and difficulties of the Internet of Things in the context of mobile computing.

Geneiatakis et al. [23] created the framework for a security and privacy risk identification for a normal home automation infrastructure with the help of off-the-shelf elements. In order to achieve this, they utilised a smart home IoT layout that facilitates users to communicate with it by a variety of devices that sustain house automation management. Authors also analysed multiple possibilities in order to find any potential security and privacy concerns for users. As part of his discussion of current RFID utilisation challenges, Khoo [24] conducted a security assessment of the RFID elements. He afterward identified hazards and concerns and explained how to resolve them or reduce risks.

In the area of green IoT-centric agricultural production, Ferrag et al. [25] discussed research difficulties related to security and privacy challenges.They started by summarising the current questionnaires that address smart agriculture before presenting a four-tier green IoT-centric agriculture layout. The threat designs against green IoT-centic farming are then divided into five groups, including intrusions into privacy, verification, confidentiality, availability, as well as integrity characteristics. Additionally, they provided a taxonomy as well as a side-by-side similarity of the most advanced approaches to secure as well as privacy-preserving innovations for IoT implementations and how they'll be modified for sustainable IoT-centic farming. Additionally, they also examined the consensus mechanism for IoT applications and privacy-focused blockchain-based alternatives, as well as how they would be modified for IoT-centric green agricultural production.

The main issues with data privacy and security were highlighted by Bertino et al. [26]. Additionally, they outlined suggestions for future research for safeguarding IoT data, such as effective as well as expandable encryption protocols, application security measures for mobile devices, as well as sensor network-specific fine-grained information packet loss investigation.

The strategy to a significant security problem was addressed and proposed by Al Shuhaimi et al. [27]. According to them, Having a quality of service where the data exchanged between the devices should be as high as possible without compromising performance is one of the key requirements for IOT. They also proposed an application model focused on Software Defined Networks. A technology known as a "software defined network" (SDN) improves network performance while using less hardware and delivers excellent security and privacy than conventional networks. The contemporary architecture design of SDN, which is appropriate for IoT as well as Ad-hoc networks, was also discussed in their research work.

Malina et al. [28] provided a thorough analysis of how well the most popular cryptographic algorithms performed on embedded devices, which are frequently found in IoT environments. On a variety of microcontrollers, intelligent tokens, as well as handheld platforms, they investigated the effectiveness of symmetric primitives like block cyphers, hash functions, randomly generated numbers, as well as asymmetric primitives like digital signature initiatives and confidentiality enhancing strategies. Additionally, they also analysed the applicability of upcoming strategies like attribute-based arrangements, group signatures, as well as homomorphic encryption strategies.

We discovered that the most relevant work to our article is concerned with IoT security through a review of the literature. As a result, our study concentrated on both the security and privacy challenges of IoT devices.

3. Security and Privacy Challenges for IoT

IoT applications have the potential to add enormous value to our everyday lives. The Internet of Things, including its newly developed wireless networks, outstanding sensors, as well as revolutionary processing capability, may represent the upcoming breakthrough in the race for a

piece of the wallet. IoT applications are anticipated to provide connectivity as well as intellectual ability to billions of ordinary items. It has already become widely used in a variety of disciplines. Industrial production, automotive, medical services, logistic support, energy, agricultural production, as well as other sectors use IoT innovations. Based on the focus of a specific IoT system, intelligent technologies can vary from basic sensors to hardware for DNA analysis. Figure 2 displays the most common IoT use applications and gadgets.

Figure 2. IoT applications in different domains

3.1. Security Challenges

Wrong access control

Only the administrator as well as the individuals they confide in their instantaneous setting should have access to the services provided by an IoT device. Moreover, equipment's security system frequently fails to adequately impose this. IoT gadgets may have a high enough degree of trust in the local area network that no additional authentication as well as authorisation is needed. Any additional hardware attached to the same network system is also assured. This becomes a challenge more so if the gadget is online because then anyone in the world could possibly use the functions and features it provides.

For gadgets of the same blueprint, the firmware as well as default configurations are typically the same. The login details for the gadget could be used to connect all gadgets in that sequence since they are known to the public, presuming that they are not altered by the user, which happens frequently. IoT gadgets frequently have a personal account or authorization level that is both externally and internally accessible. This indicates that there is no additional access control after obtaining this privilege. Multiple vulnerabilities are not covered by this one level of security.

Excessively large attack surface

Every possible interaction to a system offers a fresh set of chances for an intruder to identify and take advantage of weaknesses. A gadget can be threatened more often the more services it provides over the Internet. Threat landscape is the term for this. Among the first stages in the procedure of trying to secure a system is lowering the attack vector.

A gadget might be scheduled tasks on accessible ports that aren't strictly necessary for operating condition. By not revealing the service, an intrusion against such an unneeded service might be easily avoided. While rarely required in production, solutions like Telnet, SSH, or an error handling functionality may be crucial during advancement.

Absence of powerful encryption

A "Man-in-the-Middle" attacker can acquire all data being swapped with a client machine or backend service whenever a device interacts in plain text. Anybody with the ability to gain access to the network route among a gadget and its ending point could indeed examine the network traffic as well as possibly gather sensitive information like login information.

Even if information is encrypted, weak points might still exist if the encryption is incomplete or set up improperly. For instance, a device might not be able to confirm the legitimacy of the other entity. Although the correlation is encoded, a Man-in-the-Middle assailant can still detect it. Encryption must also safeguard sensitive information that is kept on a gadget. Lack of encryption and storing login information or API tokens in simple text on a machine are typical security flaws. Numerous different issues include the application of insufficient cryptographic techniques or the unauthorised use of cryptographic techniques.

Software security flaws

The very first stage in safeguarding IoT gadgets is to acknowledge that software includes security flaws. It may be feasible to cause capabilities in the machine that the designers had not destined due to software glitches. In some circumstances, this can lead to the assailant trying to run their own script on the system, allowing to obtain private data or launch an attack against another person. It is impossible to fully prevent security flaws when designing application. This is true of all software glitches. There are ways to prevent well-known security problems or lessen their likelihood, though. This involves using recommended procedures to prevent application flaws, like consistently validating input.

Outdated software

It's crucial to share the upgraded version of the application as soon as vulnerability is found and fixed in order to be protected from it. This implies that IoT gadgets must have updated software that is free of known vulnerabilities when they are delivered, as well as update features to fix

any security flaws that are discovered after the system is deployed.

Absence of Trustworthy Execution Setting

The majority of Internet of Things (IoT) gadgets are actually general-purpose computer systems which can run particular software. As a result, hackers are now able to configure custom applications that has features not found in the device's standard functionality. An intruder might, for instance, set up application that launches a DDoS assault. The potential for misuse of the device is reduced by limiting its features and functions and the applications it can run. One option is to limit the device's connectivity to the company's cloud service only. Due to the limitation, it is no longer capable of connecting to any destination host at random, rendering it useless in a DDoS security breach.

Code is frequently signed with an encryption algorithm to restrict the types of applications that a device can run. The machine would only run application delivered by the supplier because only they have the key to authorise application. This prevents an attacker from using a device to execute arbitrary code.

Inadequate privacy safety

Sensitive data is usually stored on consumer gadgets. The password for a wireless network is stored on devices connected to that system. A serious privacy infringement would occur if intruders were able to obtain information. IoT gadgets and associated services must manage sensitive data appropriately, safely, as well as only with the end user's permission. This holds true for both the processing and distribution of private data. The seller is crucial in terms of privacy safeguard. In addition to an external intruder, the seller or a connected party may be in charge of a privacy violation.

Seller security posture

When security flaws are discovered, the company's response heavily influences the outcome. The company's responsibilities include gathering information about potential security flaws, creating a mitigation, as well as updating deployed devices. Whether such a vendor has a procedure in place to effectively handle security problems is frequently what determines the vendor's overall security. The customer primarily interprets the company's overall security as enhanced security-related interaction with the supplier. This would probably not assist to mitigate the problem if a supplier does not offer support information or guidelines on what to do in the event of disclosing a security problem.

End users would then proceed to utilise the gadget as designed if they are unaware of any restrictions. The environment could become less secure as a consequence. Manufacturers could simplify things for clients by giving information on how frequently updates and patches are released for equipment as well as how to safely dispose of as well as sell it back the machine so that sensitive information is not transferred.

Intrusion ignorance

Whenever a system is hacked, it frequently continues to operate usually from the user's perspective. Most of the time, no extra frequency band or energy use is noticed. Most machines lack logging or notifying features that would alert the consumer of any security concerns. Users consequently infrequently learn that their gadget is being attacked or has been adversely affected, which prevents them from taking prevention action.

Inadequate physical security

Intruders could access a gadget and target the devices when they have direct access to it. Any safeguarding technology can be disregarded, for instance, by immediately reading the entire information of the memory elements. Error handling contacts that are accessible only after starting the machine may also be present, giving an attacker more options. Attacks that involve physical contact have an effect on a single system.

If a physical attack discovers an equipment key which is shared by all equipment of the same version, it may have a serious influence on many different devices. Moreover, in that scenario, researchers believe that the key sharing issue, rather than physical safety, is the more prominent issue.

Customer interaction

Distributors can promote secure device implementation through making it simple for users to customise their devices in a secure manner. Customers can be encouraged to configure secure configurations by paying careful attention to functionality, design, as well as documentation.

By understanding of the term, user interaction could be regarded by the end user, allowing the customer to assess how well a machine handles user engagement. In order to ensure that deployed security precautions are enabled and properly applied, user interaction is a crucial type. If changing the passcode is possible however the user is unaware of it or unable to use it, it is absolutely worthless.

3.2. Privacy Challenges

Information privacy is challenged in a number of ways by IoT. An introduction of the different privacy obstacles that organizations and individuals may encounter is described as follows.

Collection, use and disclosure of IoT data

IoT devices typically use sensors like microphones, motion sensors, as well as thermometers to gather information. These kinds of sensors frequently produce extremely detailed and accurate data. This level of detail makes it simple to generate extra details using machine learning assumptions as well as other analysis strategies, which can produce outcomes that are not feasible with coarser data. Additionally, sensor fusion, a technique that combines the various types of sensors or multiple devices

placed close to each other, enables the creation of more precise and detailed inferences than would otherwise be possible.

De-identification of IoT data

Huge IoT environments, like smart cities, gather all the data that can be useful for a variety of things, including policy decision-making and research. Making this data accessible to the general public digital is a common strategy to maximise its value. Datasets sensitive classified information, moreover, should never be made available to the public. Allowing people to remain anonymised by never gathering data that can recognise them is the relatively simple way to guarantee that private details is not included in a dataset. For instance, rather than using images or videos, a smart city might count pedestrians utilising IoT sensing devices that record moves.

De-identification is the method of removing private information from a dataset. Moreover, due to its strongly granular character, IoT data is frequently very challenging to de-identify. Even when grouped, longitudinal data is particularly difficult to de-identify.

Consent requirement

Consent is frequently used by institutions as justification for the use and disclosure of personal data. Moreover, obtaining a user to press "I agree" is typically not enough to obtain proper consent. Five criteria must be met for consent to be relevant: informed, specialised, current, as well as with complete capability.

Dependency on sellers

When it comes to maintaining security and privacy concerns with the help of delivering application or firmware upgrades to close security flaws, individuals and organizations who utilise IoT devices frequently rely on the supplier or producers of such equipment. They occasionally depend on supplier to make sure that the accumulated private information is adequately de-identified before it is decided to share. Manufacturers, however, frequently concentrate on particular IoT ecosystem components rather than taking into account how those ecosystems work as a whole. Manufacturers might also be predicated in countries with less stringent privacy laws. Additionally, they frequently put novel capabilities, speedy market entry, as well as ease of use ahead of privacy and security dangers. Instead of being software or hardware enterprises, consumer IoT equipment manufacturing companies are primarily consumer goods enterprises. This indicates that IoT distributors might not be sufficiently aware of privacy as well as security concerns or have the knowledge to address those concerns.

Interoperability

The rapid growth of the Internet of Things (IoT) in recent times has sparked the creation of a wide range of devices, infrastructural facilities for Application Programming Interfaces (APIs), file formats, guidelines, as well as frameworks. A person can query or inform a computer using an API to obtain a result or for a computer to interact with some other computer. Due to the fact that machines, software, as well as data through one seller frequently do not operate with those from another seller, this has led to serious interoperability problems. Data portability issues can arise from inconstant APIs as well as data formats when users' or institutions' data is kept in seller "silos" that are irreconcilable with others, making it challenging to switch supplier while maintaining data consistency.

4. Security and Privacy Taxonomy of IoT Systems

In order to design and implement the best security alternatives, configuration, as well as create secure as well as privacy IoT technologies that can assist both consumers and suppliers of IoT equipment to have a greater comprehension of the security as well as privacy attributes, it is necessary to have a comprehensive review and categorizations of the security as well as privacy prerequisites and features in IoT at the planning phase. When users talk about functionality, what we really imply is "the security as well as privacy-related characteristics, functions, processes, services, processes, as well as architectures applied within organisational information systems.

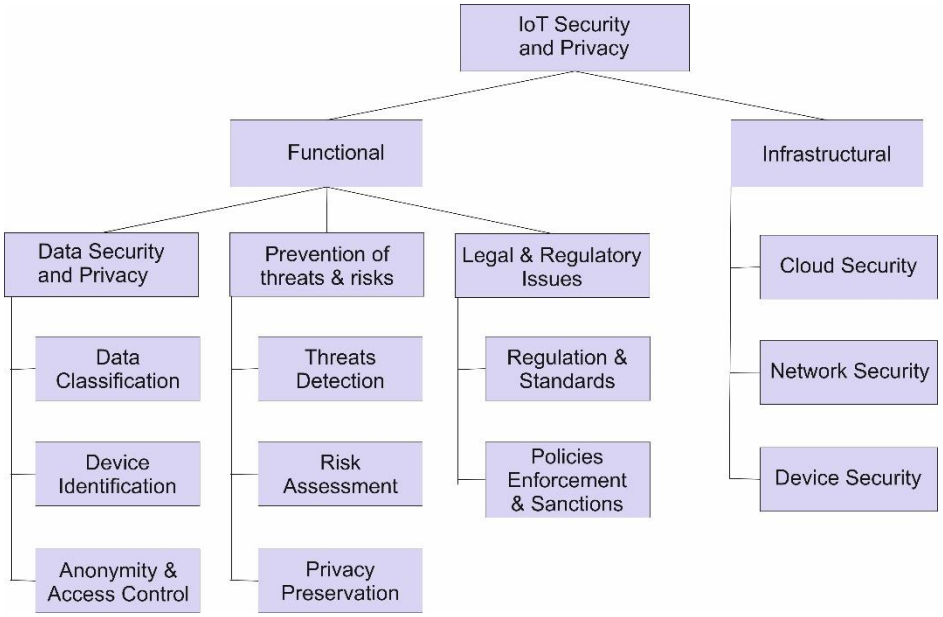

Figure 3. Taxonomy of IoT Security and Privacy

Regarding the settings in which such systems function", there are a number of basic standards, instructions, as well as methodologies [29-34] for setting up, sustaining, and enhancing an information security policy as well as safeguarding the privacy of Controlled Unclassified Information (CUI). Established IoT-related records are either provided only in readable form without specifying a blueprint or absence some security capabilities, with a special focus on privacy challenges. Such documents' layer constructions are also intricate. Even without assistance of security as well as privacy specialists, systems are frequently created. Therefore, a thorough diagrammatic framework is required [35-37]. It should also be simple to understand, including for non-experts. An extract of all IoT-related privacy and security features and functionality must be made as part of this interpretation, as well as they must be unified using a basic terminology. The rules and requirements must be incorporated in a consistent manner, and the terminology should be categorised.

The public consideration as well as mass implementation of IoT is predicated on the guarantee of privacy and security, as they gather huge quantities of sensitive information about users' identities, health, environment, location, operations, regular tasks and responsibilities, as well as certain critical data about individuals, businesses, as well as militaries. The diagram [38] in Figure 3 depicts a standard taxonomy of IoT security and privacy. For improved solutions, several privacy and security concerns associated to equipment, data, networks, as well as users in functional as well as infrastructural components of IoT must be taken into account.

5. Discussion

The IoT seeks to revolutionize our surroundings, including our houses and apartments, workplaces, and vehicles, into something smarter, more quantifiable, and friendlier. Making it simpler to play songs, set countdowns, or get information is possible with voice technology. Surveillance cameras make it simpler to keep an eye on activities both inside and outside, as well as to perceive and interact with guests. Intelligent lightbulbs could indeed make it appear as though we are home even if we're not using them, and smart switches can assist us warm up our residences before we reach home. Sensor nodes can assist us comprehend how loud and annoying or contaminated our surroundings may be when we look beyond the apartment. Many of such advancements, though, may have significant effects on our right to privacy.

The home automation is highly probable where users will first interact to internet-enabled devices, and it's another area in which the major tech firms are fiercely competing. They include smart plugs, smart bulbs, webcams, smart appliances, as well as the smart refrigerator. But there's more to smart home applications than just flaunting your enthusiasm for flashy new gadgets. Through making it simpler for household and caregivers to interact with them as well as keep tabs on how they are doing, they could be able to maintain elderly adults independent as well as in their own houses and apartments for long periods of time.

In addition to the threat themselves, managing them in the perspective of the IoT could be much more challenging. The ability to affect both online and offline systems is one of the unique capabilities of the Internet of Things. Cybersecurity threats on IoT environments may

have a lot more unanticipated effects because they can more quickly be interpreted into physical consequences. This is particularly true in the area of industrial internet of things (IIoT), in which earlier attacks have demonstrated unforeseen consequences. The use of IoT devices in the healthcare industry to wirelessly observe patients' health status has already proven to be very helpful during the COVID-19 pandemic. Cyberattack on such devices may reveal sensitive patient information or even endanger the patients' health & wellbeing.

Even though started happening when a patient monitor as well as a smart thermostat were compromised in separate attacks, malicious hackers can use weak equipment in the home automation to spy on the family, compromise security features like security systems, as well as turn equipment against their holders. The security flaws and risks covered in this essay do not have an immediate fix. Specific strategies and technologies might be needed to protect more specialised IoT systems as well as components effectively. Users can reduce hazardous situations, though, by adhering to a few best practises:

- Designate a network administrator. To lessen security vulnerabilities and complications, the network as well as IoT equipment can benefit from having a specialised administrator. They will be in responsible of making sure that IoT gadgets, including those at home, are secure. This is crucial throughout WFH configurations because IT professionals have very little responsibility over protecting home computer networks, that are now experiencing a bigger impact on the work network systems.
- Regularly check for latest update as well as fixes. Security flaws in the IoT space are a significant and enduring problem. This is due to the possibility of vulnerabilities in IoT devices at any layer. Malicious hackers continue to infect equipment utilising outdated flaws, demonstrating how long unfixed gadgets can stay online.
- Use secure and distinctive login details on all of your accounts. Utilizing complex passwords can stop a lot of hacking attempts. Password managers allow users to create powerful, one-of-a-kind passwords which they can store in the platform or applications.
- Observe how the network and devices are acting. Cyberattacks are infamously challenging to detect. Users can spot modifications that might be signs of malware infection by being aware of the device's as well as network's normal behaviour.
- Utilize technics for network segmentation. To lessen the risk of IoT-related attacks, set up separate networks for IoT equipment as well as visitors connections. Additionally, network segmentation helps isolate highly risky equipment which can not be set offline instantly and prevent the transmission of attacks.
- Use secure IoT-cloud integration as well as cloud-based alternatives. The cloud as well as the Internet of Things (IoT) are becoming more and more entangled. It's crucial to take into account how evey technology's potential consequences compare to those of the others. Cloud-based alternatives can also improve the security as well as processing power of IoT edge equipments.
- Think about security programmes and techniques. Clients who want to secure their IoT settings face significant challenges due to the restricted capability with which users may implement these initiatives. Some configurations on a gadget might be hard to customise as well as have limited access.
- Make sure to utilise GPS frequently. A few IoT machines and technologies depend heavily on GPS, that also poses security issues. Especially if they use navigation systems for manufacturing, tracking, as well as other uses, organisations must be wary of situations where GPS transmissions are congested or even spammed.

6. Conclusion

It is anticipated that the Internet of Things will expand quickly, connecting more factors of our lifestyles and obfuscating the boundaries between online as well as offline spaces. In the end, it's an instrument that could be advantageous to everyone. Moreover, the development of the IoT would then open up new opportunities for the collection of personal data and increase the volume of data collected overall. In order to make information sharing secure as well as to safeguard user data, this study intends to give the reader a basic overview of the Internet of Things, the significant privacy and security obstacles caused by its explosive increase, as well as the types of security components and solution strategies being used.

IoT technology opens up a slew of limitless perspectives and implementations. However, it is essential to deploy solutions which guarantee the security, privacy, as well as protection of IoT systems while having the least impact on overall performance, manageability, as well as functionality. Despite the fact that computer and network safety fields have provided many essential strategies and approaches over the decades, revisiting and expanding such methods and strategies to confront the specific characteristics of IoT systems presents many technological and scientific issues. Without a reason to suspect, access control as well as exposed assistance is the main security issues. IoT machines should also use best practises security safeguards like encryption. By offering documentation and communicating with customers and security experts, distributors can encourage the secure utilisation their products. Gadgets must be physically managed to secure to render it more difficult for intruders. Subsequently, if a system is breached, it must dismiss the attacker's programmes and alert the user to a problem.

Because of the interdependent character of the sensing devices, the limited resources, as well as the architecture design used in IoT systems, traditional security components cannot be used. Strong network safety infrastructural facilities are necessary to prevent unauthorised use of user information, protect their privacy, as well as mitigate privacy and security attacks.

Consequently, it is crucial to spend more in projects involving this as well as other cutting-edge technology. To enhance the business operations and function in today's networked society, we need a thorough IoT framework, deep learning, machine intelligence, and embedded devices. Humans can benefit from the wirelessly connected ecosystems' smart capabilities, characteristics, and efficiency by making the most of this powerful advanced technology.

Acknowledgements.

The authors gratefully acknowledge the support from Department of Computer Science & Engineering, Azad Institute of Engineering & Technology, Lucknow, Uttar Pradesh, India.

References

[1] Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers.

[2] Abdel-Basset, M., Manogaran, G., Mohamed, M., & Rushdy, E. (2019). Internet of things in smart education environment: Supportive framework in the decision-making process. *Concurrency and Computation: Practice and Experience*, *31*(10), e4515.

[3] Ortiz, A. M., Hussein, D., Park, S., Han, S. N., & Crespi, N. (2014). The cluster between internet of things and social networks: Review and research challenges. *IEEE internet of things journal*, *1*(3), 206-215.

[4] Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), 2233-2243.

[5] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1-31.

[6] Algarni, A. (2019). A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access*, *7*, 101879-101894.

[7] Haque, N. I., Rahman, M. A., Shahriar, M. H., Khalil, A. A., & Uluagac, S. (2021). A novel framework for threat analysis of machine learning-based smart healthcare systems. *arXiv preprint arXiv:2103.03472*.

[8] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2019, October). Healthguard: A machine learning-based security framework for smart healthcare systems. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 389-396). IEEE.

[9] Khatri, S., Alzahrani, F. A., Ansari, M. T. J., Agrawal, A., Kumar, R., & Khan, R. A. (2021). A systematic analysis on blockchain integration with healthcare domain: scope and challenges. *IEEE Access*, *9*, 84666-84687.

[10] Ansari, M. T. J., Agrawal, A., & Khan, R. A. (2022). DURASec: Durable Security Blueprints for Web-Applications Empowering Digital India Initiative. *EAI Endorsed Transactions on Scalable Information Systems*, e25-e25.

[11] Raval, M., Bhardwaj, S., Aravelli, A., Dofe, J., & Gohel, H. (2021). Smart energy optimization for massive IoT using artificial intelligence. *Internet of Things*, *13*, 100354.

[12] Samann, F. E. F., Zeebaree, S. R., & Askar, S. (2021). IoT provisioning QoS based on cloud and fog computing. *Journal of Applied Science and Technology Trends*, *2*(01), 29-40.

[13] Shahzad, Y., Javed, H., Farman, H., Ahmad, J., Jan, B., & Zubair, M. (2020). Internet of energy: Opportunities, applications, architectures and challenges in smart industries. *Computers & Electrical Engineering*, *86*, 106739.

[14] Butpheng, C., Yeh, K. H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry*, *12*(7), 1191.

[15] Ansari, M. T. J., Pandey, D., & Alenezi, M. (2018). STORE: Security threat oriented requirements engineering methodology. *Journal of King Saud University-Computer and Information Sciences*.

[16] Bhatt, S., & Bhushan, B. (2022). Cyberattacks and Risk Management Strategy in Internet of Things Architecture. In *Artificial Intelligence and Cybersecurity* (pp. 51-68). CRC Press.

[17] IOT Security Statistics (2022): What you should know. Intersog. (2021, December 1). Retrieved June 25, 2022, from https://intersog.com/blog/iot-security-statistics/

[18] Sava, J. A. (2022, April 19). IOT Security Market Size Worldwide 2016-2025. Statista. Retrieved June 25, 2022, https://www.statista.com/statistics/993789/worldwide-internet-of-things-security-market-size/

[19] Ansari, M. T. J., Al-Zahrani, F. A., Pandey, D., & Agrawal, A. (2020). A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Medical Informatics and Decision Making*, *20*(1), 1-13.

[20] Ansari, M. T. J., Baz, A., Alhakami, H., Alhakami, W., Kumar, R., & Khan, R. A. (2021). P-STORE: Extension of STORE methodology to elicit privacy requirements. *Arabian Journal for Science and Engineering*, *46*(9), 8287-8310.

[21] Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. A. (2017). A review on internet of things (IoT): security and privacy requirements and the solution approaches. *Global Journal of Computer Science and Technology*.

[22] Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. U. (2020). Security analysis of IoT devices by using mobile computing: a systematic literature review. *IEEE Access*, *8*, 120331-120350.

[23] Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017, May). Security and privacy issues for an IoT based smart home. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1292-1297). IEEE.

[24] Khoo, B. (2011, October). RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 709-712). IEEE.

[25] Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE access*, *8*, 32031-32053.

[26] Bertino, E. (2016, March). Data Security and Privacy in the IoT. In *EDBT* (Vol. 2016, pp. 1-3).

[27] Al Shuhaimi, F., Jose, M., & Singh, A. V. (2016, September). Software defined network as solution to overcome security challenges in IoT. In *2016 5th International Conference on Reliability, Infocom*

Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 491-496). IEEE.
[28] Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, *102*, 83-95.
[29] Slama, D., Puhlmann, F., Morrish, J., & Bhatnagar, R. M. (2015). *Enterprise IoT: Strategies and Best practices for connected products and services*. " O'Reilly Media, Inc.".
[30] Collins, T. (2017). A methodology for building the Internet of Things. *Retrieved August*, *21*, 2021.
[31] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2018). A risk assessment methodology for the Internet of Things. *Computer Communications*, *129*, 67-79.
[32] Perumal, S., Norwawi, N. M., & Raman, V. (2015, October). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)* (pp. 19-23). IEEE.
[33] Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In *Architecting the internet of things* (pp. 1-24). Springer, Berlin, Heidelberg.
[34] Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., & Eschert, T. (2017). Industrial internet of things and cyber manufacturing systems. In *Industrial internet of things* (pp. 3-19). Springer, Cham.
[35] Galbusera, F., Casaroli, G., & Bassani, T. (2019). Artificial intelligence and machine learning in spine research. *JOR spine*, *2*(1), e1044.
[36] Lemos, A. L., Daniel, F., & Benatallah, B. (2015). Web service composition: a survey of techniques and tools. *ACM Computing Surveys (CSUR)*, *48*(3), 1-41.
[37] Jallow, A. K., Demian, P., Anumba, C. J., & Baldwin, A. N. (2017). An enterprise architecture framework for electronic requirements information management. *International journal of information management*, *37*(5), 455-472.
[38] Muzammal, S. M., & Murugesan, R. K. (2018, October). A study on leveraging blockchain technology for IoT security enhancement. In *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)* (pp. 1-6). IEEE.