Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 1977–1989
DOI : 10.47974/JDMSC-2073

Addressing applications and security issues in the Internet of Things (IoT) : A comprehensive review

Pallavi Pareek *
Surendra Yadav †
Department of Computer Science
Vivekananda Global University
Jaipur 302017
Rajasthan
India

Surendra Singh Choudhary §
Department of Computer Science
Sri Balaji College of Engineering and Technology
Jaipur 302013
Rajasthan
India

Abstract

The Internet of Things IoT connects human beings, smart devices, smart systems and a large amount of data changing the world network. With the number of interconnected devices increasing, data protection and communication security become difficult. The number of IoT devices has increased over time, mostly in two sectors: industry and residences. What was previously presented is a complete ecosystem for Amazon Echo devices and the Alexa Voice Service. That is why Apple, Microsoft, and Google have all done the same. Platform providers are also accountable for device security since the platform they offer is closed and operates as a standalone one. Cybersecurity in manufacturing industries and related firms is the main focus of this paper. Industry sectors such as production and processing, oil and gas, refining, medicine, food and beverage, and water treatment are becoming interested in effective security solution as more of the devices and equipment getting connected to Internet. Manufacturers, especially operators of large plants, as well as gadget makers, have to guard their metal and other physical infrastructure against cyber threats. These businesses

* *E-mail:* **pallavi19586@gmail.com (Corresponding Author)**
† *E-mail:* **syadav66@gmail.com**
§ *E-mail:* **Ssc_jaipur@yahoo.com**

generate distinct kinds of data and utilise distinct IoT environments, and threat management and compliance become complicated.

Subject Classification: *Primary 68M12, Secondary 90B18.*

Keywords: *IoT, Applications, Security issues and network.*

I. Introduction

IoT is currently the most rapidly developing technology that has a clear impact on social life and also in the corporate world due to its recent rapid development and variety of offered services [1]. IoT-end connected devices are fast going global, and IoT services are also going global. That success has not gone unnoticed and there are also more threats and attacks being directed towards IoT services and things [9].

IoT is an idea that can significantly revolutionize the way people communicate with the help of technology. In some works of science fiction, the future envisioned is one in which every device contained within one's environment is in itself a node within this single, global network. However, IoT is not only influencing the nonfiction world – it's taking over the world. Subsequently, IoT devices are finding their way into the market. Smart connected devices will have the largest impact on our daily lives in our smart homes where they are moving from working stations [2]. The majority of smart home equipment will be common, innocuous items like toasters and kettles. There isn't much a hacker can do to bother you, even if these gadgets are penetrated and hacked, except for spoiling your breakfast. Since the Internet of Things is still in its early stages of growth, the market is now concentrating on its vertical sectors. However, the Internet of Things cannot be seen as a single entity, platform, or even technology. More attention must be paid to interfaces, platforms, mobile apps, and common/dominant standards if the IoT is to expand at the predicted fast rate [3].

In the education sector, the Internet of Things (IoT) is already beginning to automate the traditional educational system. Interactive smart classrooms are encouraging student participation and learning, and different student monitoring systems and automatic attendance might contribute to the safety of schools. For underdeveloped nations, the introduction of internet-enabled remote classrooms will mark a significant advancement since they may penetrate locations where conventional school infrastructure cannot be established. Through automated process

controls, internet-enabled manufacturing and industrial facilities are producing outcomes that set companies apart and increase their safety and efficiency [2]. Plant and energy optimisation, health and safety monitoring, and security management are increasingly dependent on advanced sensor networks and powerful microcomputers. Numerous services provided by financial services currently make use of the Internet. The next wave of IoT-enabled goods and exponential advancements in digital infrastructure may propel the financial industry's expansion. Goods like smart wearables and smart monitoring devices will allow consumers to manage their finances and assets more effectively. IoT-enabled devices may lead to an increase in data use for telcos, which would increase ARPU (average revenue per user). However, telcos would also need to address issues like infrastructure security and privacy [4]. These emerging technologies provide enormous IoT cybersecurity risks in addition to their astounding potential. Attacks on Internet of Things devices have become much more frequent and sophisticated over the last several years. A number of cybercrime opportunities and ways into the interconnected people, devices, and organisations of the digital age are created by the Internet of Things. The risk 'horizon' of an organisation is, in fact, just one more element in a started, often contradictory, and not immediately transparent universe of risk. Some of these risks are from strange people and rise in the extreme. This article examined several IOT security issues [5]. This paper's primary contribution is an overview of the IoT security concerns as they stand right now.

II. Internet of Things (IOT)

Some of the components in the Internet of Things include computers devices, physical machinery, items, animals and people that may or may not engage in communication over a network without control or interference of machines and computers. These entities have their own unique identification number or UID. IoT "things" are as follows such as a human with a heart checker; a farm animal with a integrated transponder; and, an automobile with low-tire pressure sensors. IoT can be defined as the connection of every IP-enabled device with the ability to send and receive information over a network.

IoT optimizes operations, organizational processes, customers' buying habits, and organizational value throughout industries. Internet of Things (IoT) was developed in computer sciences to make appearance on the course of other appliances we use in our daily lives. RFID might mean

different senor technologies, wireless communication systems and QR codes.

III. Characteristics of the internet of things (IOT)

Among the most well-liked features of the Internet of Things are:
(a) Intelligence (b) Connectivity (c) Dynamic Nature (d) Enormous scale (e) Sensing (f) Heterogeneity (g) Security

(a) Intelligence: The IoT obtains its intelligence from a combination of devices, codes and applications. In the context of the Internet of Things, ambient intelligence enhances its capability to compute how objects can respond appropriately to a certain situation and how it can support objects in the accomplishment of certain tasks. Nevertheless, the use of smart technologies characterizes the IoT and although these technologies are intelligent, the intelligence found in IoT is simply the means of communication between entities; the methods of interaction may only be through graphical user interfaces and/or conventional input-output input methods where users and entities may interface with the actual devices.

This intelligent spark is the software and hardware in makes a product experience intelligent. Compare Misfit's non-smart fitness tracker known as the Misfit Shine to Nest's smart thermostat. Calculating duties in the Shine experience occurs in two settings: smartphone and the cloud. Compared to the AI that makes them intelligent, the Nest thermostat has more computing abilities.

(b) Connectivity: The ability to connect things to the Internet and with one another is the driver of the Improved Internet of Things where we attach commonplace devices in the process. As basic object-level communications assist in building a hub of intelligence for an IoT network these things need to be connected. It makes the objects amenable to connectivity through networks. This connection may break new markets for the Internet of Things with the networking of smart objects and apps. In the context of the Internet of Things, connectivity is not as simple as installing a WiFi module to claim that the product is connected [6]. Connectivity makes network compatibility and accessibility possible. Appending to a network is called availability while sharing the ability to build as well as apply data is known as interconnection. If this rings a bell, there is a good reason – Metcalfe's Law applies to the IoT.

(c) Dynamic Nature: The purpose of the IoT is to gather information from its environment and make these changes possible to achieve. These

devices' dynamic states include, for example, sleeping mode, waking mode, connected or not connected, and other devices. In parallel to the state of the device a change determine the availability of how many devices there are.

Device states may vary over time, e.g. when they are asleep or wake up, when they are connected or not, in what mode they are being used, for example in a car or walking. In addition, it is also possible to foresee that the shipped quantity of devices might differ dynamically.

(d) Enormous scale: There will be far more gadgets than smart devices currently connected to the Internet that require control and interconnectivity. These increase the requirement of managing the data produced by these devices and knowing it for use in applications. Gartner (2015) in his estimation study supports the extensive reach of IoT simplifying that 5.5 million new things will be connected daily and by the end of 2016, the number of connecting things globally would rise to 6.4 billion, up from 5 billion in 2015. So the latest perception, considering all the links, is that by the year 2020, there will be 20.8 billion linked devices.

By the year 2005, at least ten times as many devices will require being managed and communicated and are currently connected to the Internet. The management and subsequent analysis and preparation of the generated data for application use will be even more critical. This has to do with data management or more correctly; semantic data management.

(e) Sensing: Nevertheless, it is rather difficult to imagine how the Internet of Things could exist without sensors: how can objects monitor and record such changes in the atmosphere, report on or talk to its condition? Due to sensing technology, it is possible to build skills which meant to reflect an adequate level of understanding of the surrounding physical context and the actors in it. Thus even if sensory data is merely the analog input from the physical world it may one day give us a fundamental understanding of our spectacularly designed universe.

It reminds us of how little we pay attention to the ability or the lack of it to see the world and the people it consists of. It becomes now possible for us to design and deploy experiences that would reflect our understanding of the physical environments and the individuals populating it through sensing technology. This is merely the analog of the physical world input, but, it may help us gain a profound understanding of our almighty reality.

(f) Heterogeneity: The main feature of the Internet of Things is its heterogeneity in its general sense. IoT devices may interact with other devices or service domains through different networks, and the IoT

devices are developed based on different hardware platforms and networks. There is a need for the IoT structure to facilitate direct network communication between heterogeneous networks. In the Internet of Things, various objects and their contexts require scalability, flexibility, extensibility, and interoperability. IoT is characterized by the heterogeneity of its components, namely its devices are based on different hardware platforms and employ different networks.

(g) Security: IoT devices are innately vulnerable to security threats since they come with open access. While everyone is occupied with new opportunities provided by the Internet of Things, with new possibilities, convenience, and other benefits, it is wrong to turn a blind eye to the security problems that arise with the help of the Internet of Things. First of all, IoT poses a great number of privacy and transparency questions. It has been stated that a new security perspective is required to protect endpoints, networks, and the data that is transferred between them.

IV. Use of the internet of things (IOT)

The following are some practical Internet of Things (IoT) applications: (Figure 1)

(a) Connected Health (b) Smart City (c) Connected Cars (d) Smart Home (e) Smart Farming (f) Smart Retail (g) Smart Supply Chain

(a) Digital health, telemedicine, and other forms of connected health IoT have several applications in the healthcare sector right from equipment integration, and standard & high-end smart sensors to health monitoring. It might improve the doctors' approach to the patient and his/her safety and stability. Medical Care IoT may improve both patient satisfaction and the level of happiness as more frequent interactions between patients, as well as clinicians may occur. IoT in healthcare brings in new tools which has the latest technology added in the IoT ecosystem that helps to create better healthcare delivery; from the surgical robots to the fitness wearable. IoT dramatically improves healthcare service and it costs less than other service-providing industries for both the customers and the professionals, [9].

This is still tethered connected healthcare and one of the Internet of Things sleeping giants. The concepts of the enforcement of an almost integrated healthcare system and smart inverted continuing medical devices pose not only profound opportunities in the commercial development and innovation perspective but also the sense of improved welfare of the targeted population. Analyzed research indicates that IoT in

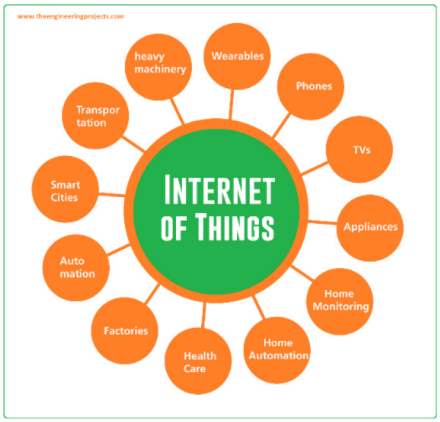

Figure 1

Use of IoT

Source: [16]

healthcare will be massive in the next few years. The purpose of IoT in healthcare lies in the fact that people can wear several interconnected devices and improve their lives. This information will assist in carrying out a differential diagnosis of each individual by developing unique ways of approaching diseases and preventive causes. The following video is a real-world demonstration of how IoT is likely to revolutionize healthcare and medical support [10].

(b) Smart City Another powerful IoT application that is interesting to people all over the world is smart cities. Some areas of IOT application in smart cities include smart transportation systems, smart water supply systems, smart energy management systems, smart surveillance systems, Smart Urban Security Systems, and Intelligent Environmental Monitoring Systems. Floats and problems of the city's inhabitants like pollution, congestion in streets, and lack of energy shall be addressed by IoT [7].

When sensors of parking spots are fitted, and the use of the internet, it becomes possible to identify open parking lots across the entire city. Besides, the sensors detect general failures, installation failures with the electrical system, and meter tampering [7].

(c) Connected Cars The objective of automotive digital technology has been to improve the internal operating systems of the vehicle. But these days, more efforts are being made towards enhancing the feel inside a car. A connected automobile is one that self-optimizes using an internet connection and sensors installed within the vehicle to perform maintenance,

work, and provide entertainment. Most of the large car manufacturers and a few start-ups are working on linked vehicle technologies. Industry leaders including Tesla, BMW, Apple, and Google are trying to bring the next breakthrough in the automotive industry.

Connected automobile technology refers to the vast and diverse conglomeration of several sensors, antennas, embedded software, and technologies used in communication to move in thereby complex world. It is responsible for making choices with speed, access to accurate information, and reliability. It must also be trustworthy [10]. As humans hand over fully the responsibility of steering and breaking from the human-operated or self-driving cars that are already being tested on our roads, these needs will become even more vital.

(d) Smart Home The context of providing relative comparisons of years of growth in technology penetration, a range of new products, services, and experiences related to smart homes gradually appeared. It is quite apparent that the emergence and domination of smart homes warrant the candidate in terms of business promotion. We have seen over $2.5 billion channelled towards the growth of smart home business however the amount continues on an upward trend [9].

House ownership, especially the first time for a homeowner, requires the largest outlay in life. With the increased marketing efforts to produce these products, they are said to result in cost, energy, and time savings. New technologies and, consequently, smart home inclusionary products such as Nest, Ecobee, Ring, and August amongst others are likely to be within reach of every household.

(e) Smart Farming The niche of smart farming in IoT applications is usually overlooked. On the other hand, IoT devices can supervise all of this and change the operational procedures for farmers as most farming practices are remote due to the large herds. Nonetheless, this idea has not been paid much attention. Nevertheless, it remains one of the prominent applications of IoT that needs to be addressed. More specifically, smart farming development prospects are of great interest in the countries, which are agricultural exporters [7].

(f) Smart Retail Retailers have been adopting IoT solutions and applying IoT system-integrated applications for purposes that improve the store outlets' sales, losses, stocks, and customers' comfort and satisfaction. IoT enables physical merchants to create more offers and services to customers than actual online rivals [8]. They can regain their market share, lure the customers in and it'll become easier to stimulate them to buy a bigger ticket item.

IoT is great for employment in the retail sector as the final result. Hridi explains that IoT adopted by retailers can lead to consumer engagement and enhanced in-store experience. Smartphones will open the possibility for retailers to communicate with their customers even when the consumers are not in the stores. Customer service can be enhanced by interacting with the Beacon technology and the smartphones as observed by retailers [8].

(g) Smart Supply Chain: For a few years now, supply networks have been becoming more intelligent. Providing solutions for issues like monitoring products while they are traveling or on the road, or assisting suppliers in exchanging inventory data, are a few of the well-liked offers. Factory equipment with integrated sensors may send data about many factors, including temperature, pressure, and machine utilization, via the use of an Internet of Things-enabled system [8]. To maximize performance, the IoT system may also process workflow and modify equipment settings.

V. Security challenges facing IoT

The protection of Internet of Things devices from intrusion is referred to as IoT security (Figure 2). Everyone who owns a company understands that he or she needs to install antivirus software to protect their PC or telephone but at the same time, they often fail to realize that IoT gadgets are also potential threats.

Internet of Things gadgets are ubiquitous. Almost everything we see is connected to the internet today including refrigerators, automobiles, and surveillance cameras talk of production lines. The Internet of Things is growing at a very high speed; it is forecasted that by 2022; there will be over half a billion IoT sensors and devices Juniper Research. Highlighted above are various aspects of the Internet of Things, IoT devices' usage is rapidly growing since they offer great profitability for business over time, not to mention the beneficial features consumer IoT devices confer [11]. For example, Harley-Davidson has increased its net margin by 19% and reduced expenses by 7% after redesigning its production line in York, Pennsylvania "smart factory" and installing IoT devices at every stage of production.

(a) Data Integrity: A connected world of billions of gadgets is the Internet of Things. If any of the data points in the whole set being sent and transmitted between the sensor and the main server are to be manipulated, then the manipulations are overall accomplished. They should ensure

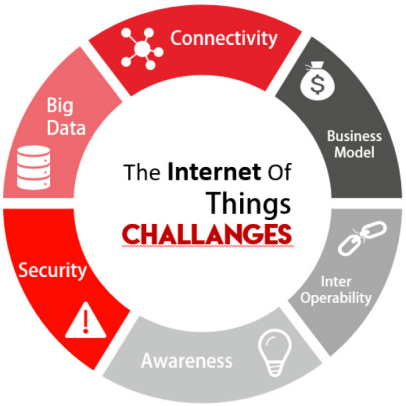

Figure 2

Challenges

Source: [15]

integrity by employing the theory: of digital signatures and decentralized distributed ledgers [11].

(b) Encryption Capabilities: The process of converting data in the two forms is equally continuous. The Internet of Things is still not able to process data through the container's intruder sensors. Firewalls and isolating the devices onto two separate networks may indeed prevent brute force attempts.

(c) Privacy Issues: The main concept of the Internet of Things is exchanging data across platforms, devices, and users. Smart devices are for data gathering to make it effective, and experienced, for decision-making and providing better services. Thus, the protection has to be total where the data is going to end up [12].

(d) Common Framework: Since there isn't a single framework, each manufacturer is responsible for maintaining privacy and security on their own. Reusability of code may be accomplished after a common, standardized framework is put into place, allowing the individual efforts to be combined and used in an expanding way.

(e) Automation: Businesses will eventually have to cope with an increasing number of IoT devices. Managing this massive volume of consumer data might be challenging. It is an undeniable reality that all it takes to bring down the whole data infrastructure is a single mistake or algorithmic trespass [13].

(f) Updation: For the millions of devices, updates are required frequently, but only a section allows OTA updates, which means that device upgrades are still a thing. The procedure for tracking the available update and applying them on various devices is complex and time-consuming. This makes this procedure potentially mundane and elaborate and any mistake that might be made would lead to the creation of vulnerabilities. Safety Priority should now be given to investments in network and infrastructure security, but this is not the case. Millions of data points are used in IoT, and each one has to be safeguarded. It is true that multi-layer security, or security at every level, is required [14].

VI. Conclusion

In the case of the IoT architecture, all seven layers are under threat. Consequently, the following security risks and requirements are in place. Currently, the research activities for IoT are mainly in the area of authentication and access control schemes; yet to achieve the gradual integration of the IoT topology as outlined in the progressive mash-up model, new networking such as IPv6 and 5G need to be established as technology is rapidly evolving. The specific focus of this chapter was to raise awareness of the more critical IoT security threats, considering security threats and attacks and their defenses. This is mostly the case since most of the IoT devices turn into soft objectives due to vulnerabilities; users may not even know they have a device under attack. Some of the security criteria identified in this chapter are information privacy, data integrity and user authentication. Further, this paper presents a literature review of some of the IoT applications as listed below. The purpose of this article is to enhance the understanding of security specialists of various threats that have been posed by the threats posed by the different agents such as organisations and even intelligence services by detailing some critical IoT security issues.

References

[1] H. Tahir, A. Kanwer, and M. Junaid, "Internet of Things (IoT): An overview of applications and security issues regarding implementation," *Int. J. Multidiscip. Sci. Eng.*, vol. 7, no. 1, pp. 14-22 (2016).

[2] 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, p. 383 (2017).

[3] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards security on internet of things: applications and challenges in technology," Procedia Computer Science, vol. 141, pp. 199-206 (2018).

[4] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of things security: challenges and key issues," *Security and Communication Networks*, vol. 2021, no. 1, p. 5533843 (2021).

[5] L. S. Sayana and B. K. Joshi, Security issues in internet of things. Uttarakhand: ICFAI (2016).

[6] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems,* vol. 67, pp. 423-441 (2018).

[7] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491-498 (2019).

[8] S. Rana, S. Hossain, H. I. Shoun, and M. A. Kashem, "An effective lightweight cryptographic algorithm to secure resource-constrained devices," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11 (2018).

[9] C. Henke, "What Is IoT Security? Risks, Examples, and Solutions," emnify. [Online]. Available: https://www.emnify.com/iot-glossary/iot-security#authorbio. [Accessed: 10-Jun-2024].

[10] R. Mohanakrishnan, "Top 10 Applications of IoT in 2022," Spiceworks. [Online]. Available: https://www.spiceworks.com/tech/iot/articles/top-applications-internet-of-things/. [Accessed: 10-Jun-2024].

[11] B Pragathi, DK Nayak, RC Poonia," Mitigation of power quality issues for grid-connected photo voltaic system using soft computing techniques," *Journal of Interdisciplinary Mathematics*, Vol. 23 (2), pp. 631-637 (2020).

[12] A. Parashar and S. Rishishwar, "Security challenges in IoT," in 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), pp. 446-449 (2017).

[13] L. A. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Applied Sciences,* vol. 10, no. 12, p. 4102 (2020).

[14] S. I. Al-Sharekh and K. H. Al-Shqeerat, "Security challenges and limitations in IoT environments," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 193-199 (2019).

[15] W. Technologies, "6 Main Challenges Facing IoT," Medium. [Online]. Available: https://medium.com/@winix/6-main-challenges-facing-iot-b6055bdf6782. [Accessed: 10-Jun-2024].

[16] D. Watson, "What is IoT (Internet of Things)? Definition, Meaning, Devices & Applications," The Engineering Projects. [Online]. Available: https://www.theengineeringprojects.com/2021/03/what-is-iot-internet-of-things-definition-meaning-devices-applications.html. [Accessed: 10-Jun-2024].

Received March, 2024