Internet of Things Based Smart Environment: Threat Analysis, Open Issues, and a Way Forward to Future

Atharva Deshmukh
Department of Computer Engineering
Terna Engineering College
Navi Mumbai, India
atharva1525@gmail.com

Amit Kumar Tyagi[0000-0003-2657-8700]
School of Computer Science and Engineering,
Vellore Institute of Technology, Chennai, 600127,
Tamiladu, India.
amitkrtyagi025@gmail.com

N Sreenath
Department of Computer Science and Engineering,
Puducherry Technological University, Puducherry, India
nsreenath@pec.edu

Shraddha Jathar
Department of Computer Engineering
Terna Engineering College
Navi Mumbai, India
shraddha14.jathar@gmail.com

Abstract—**Security is a key concern in the Internet of Things Based Smart Environment research. The data generated by smart IoT devices must be dealt with securely. Nowadays with the growing number of smart IoT devices, current systems and security standards cannot guarantee that they will operate successfully in all scenarios. This paper gives a detailed overview of Issues and a way forward to the future related to the IoT Based Smart Environment because of the fast surge of IoT devices users, as well as the variety and complexity of these items and their networks, authentication has become a difficult problem. Other restrictions, such as limited processing capabilities, and restricted storage as well as power in some cases on some of the small embedded devices, make it difficult to execute complicated cryptographic algorithms.**

Keywords-component; Internet of Things; Smart Environment; Smart Grid; Intelligent Transport Systems; Big Data; cloud computing;

I. INTRODUCTION

Computer technology has advanced to the point where small sensors and processors may be integrated into common things that we use in our daily life because of rapid advancements and miniaturization of computer technology. The Internet connects us to the physical world through smart home security systems, self-driving smart cars, wearable health monitors, and biometric cybersecurity scanners. These new applications of Internet of Things (IoT) give humongous opportunities, however, they come with some inescapable risks. The Internet of Things permits human beings to understand and manipulate items, bearing in mind a greater direct connection among the bodily global and computer-primarily based totally systems. IoT has the potential to bring a new wave of automation in different designing domains, which also includes production and energy management like Smart Grid, in addition to healthcare control and city life. In the coming years, the 5G network would act as a base infrastructure for all the IoT devices as it would provide massive data connectivity and a massive device capacity along with zero latency, this would definitely reduce the current gap between machines and people. But IoT also creates security problems due to its capabilities like pervasive, continuous, and fine-grained data collecting with data control capabilities.

A. *Advantages of Cloud-driven Internet of Things*

Leveraging IoT technologies by migrating them from centralized local server systems to distributed cloud architecture can be advantageous in a variety of applications. With this design, we can process queries in real-time with lower transmission costs, lowering processing overhead even more.

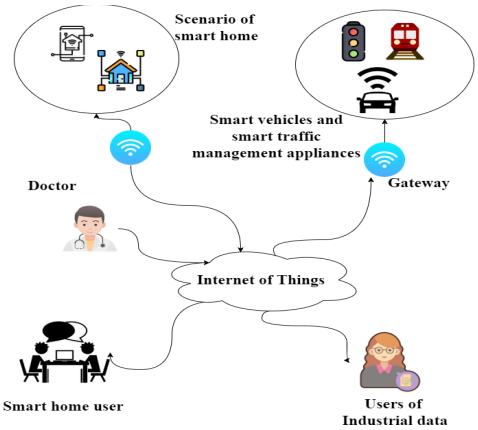

Figure 1. A generic IoT environment for Smart Era

The data can be accessed from practically anywhere in the globe if it is stored and processed on a cloud server, which also means it is not constrained by any infrastructure as well as networking limits. One of the most significant benefits of hosting your IoT system on the cloud is the ease with which it can be scaled. Large initial upfront costs in the case of an in-house Internet of Things solution might be disappointing but cloud-driven IoT can provide a pay-as-you-go model which can be highly cost-effective. We'll go over a few more benefits of cloud-based IoT versus conventional IoT in the next sections. Figure 1 depicts an IoT based Smart Environment.

B. *Big Data's Role*

In Big Data analytics, the IoTs assists enterprises in extracting data for improved business insights. Better business insights aid in making more informed decisions that yield a good return on investment. As previously stated, the cloud can be an ideal platform for storing and processing the data produced by IoT

978-1-6654-8035-2/22/$31.00 ©2022 IEEE

devices. Cloud computing platforms are recommended for handling big data generating using IoT devices. The following is the role of an IoT-based big data environment in the cloud:

- Big Data and Cloud Data are inseparable because the Cloud architecture enables storage, real-time processing, and Big Data analysis at scale and speed.
- Without the need for human interaction, IoT devices can connect with one another and collect and exchange real-time data.
- Data created from smart IoT devices in an IoT ecosystem may rise exponentially over time.
- Exabytes of data may be collected in the future, which must be processed swiftly and rationally in order to make the best judgments possible.
- The analysis of data generated by smart IoT devices is constrained by traditional data processing technologies, storage systems, data warehouses, and relational databases.
- Traditional methods are prohibitively expensive when a user is dealing with large amounts of data.
- Most notably, traditional approaches are unable to handle data efficiently and quickly, this is very critical for processing data in real time in deployment fields where different IoT devices are installed.
- IoT requires new tools and approaches that have the capacity of storing as well as analyzing humongous data.
- Such tools and approaches make the process of acquiring, transferring, finding, analyzing, and visualizing the massive amounts of data created by smart IoT devices easier.

II. Motivation and Background

Several research projects have been undertaken in order to combine IoT with smart environments. The Internet of Things technology allows the Internet to connect with actual devices in the real world [1]. There would be around 35 billion IoT devices worldwide by the end of 2021. Short-range wireless communications, Radio Frequency Identification (RFID), sensor networks, and real-time localization are all are very common nowadays, this makes the Internet of Things a reality [2]. Today we're going through a paradigm change, where commonplace devices are becoming more linked and intelligent. However, because human understanding, as well as experience of working with interconnected smart things and smart systems, has not progressed at the same rate, this poses significant technological, privacy, and security concerns [3]. A diverse group of academic and industrial researchers, businesses, government organizations, etc suggested that this technology should be investigated from three different perspectives: user experience, engineering design, and scientific theory [4]. AI can be implemented in all areas where IoT devices are used including power and traffic management, industrial production, remote medical treatment, agriculture, building, smart home, environment management, and so on, in order to create a smart networked society in which resources are effectively used, resulting in a favorable impact on the people. All of this cutting-edge IoT development creates new security challenges and research gaps that must be addressed [5]. IoT security must be addressed in light of the features of the IoT ecosystem in which it is used.

A. Internet of Things Security Vision

IoT devices are the main driving force behind a smart future in which things play an important role in our daily lives [6]. The wireless sensors or the Radiofrequency Identification (RFID) tags are the most common connected nodes. Although Transport control protocol (TCP) / Internet protocol (IP) is mostly used protocol for Internet communication, Mostly IoT devices are connected to a central hub through which all the data is sent to a dedicated server or a cloud using a short-range communication protocol. Near field communication, 6LoWPAN, ZigBee, IEEE 802.15.4, IEEE 802.15.4, Wi-Fi, and Bluetooth are some of the short-range communication technologies [7]. The sensing layer contains a physical IoT device or multiple devices that sense and share various recorded parameters from surroundings. Attackers can retrieve sensitive information from these devices if they gain control of them [8]. The data is exchanged between the application layer and the sensing layer is done via the network layer, which uses internet infrastructure. Application layer is responsible for data storage, analysis, and presentation to the end-user. Different entities are in charge of managing and maintaining the software and hardware at these various layers. One supplier, e.g., may maintain the physical hardware at the sensing layer. The network layer might be controlled by another network provider, while the cloud provider can host the data of the application layer and access it by software developed by a third party [9]. Secure data transfers of data between all of these entities are critical at the communication level [10].

B. Importance of Internet of Things Cloud-driven Big Data

When you combine Big Data, IoT, and Cloud, you may achieve the most effective and efficient communication, connection, and data transference across devices [11]. Cloud computing is essentially a facilitator. It also provides a hosting platform for Big Data and IoT along with data analytics [12]. The key advantage of employing Cloud Computing in conjunction with IoT and Big Data is that it is a scalable, trustworthy, and flexible tool for enterprises. [13] The interdependence of Cloud Computing, Big Data, and IoT is a synergistic interdependence that provides your organization with actionable insights via performance and analysis reports. According to a report, the Internet of Things has created around 4.4 trillion GB of data by 2020 [14]. When enterprises collect data for analytical purposes, IoT serves as a primary source of such data, and here is where the function of big data in IoT enters the picture. [15] Big data analytics is developing as a critical component for evaluating IoT-produced data from connected devices, which aids in taking the initiative to enhance decision-making.

III. TAXONOMY

The taxonomy of the IoT-based smart environment is depicted in the diagram below. The taxonomy developed is based on the following parameters:

- **Communication Enablers**: Wireless technologies used to communicate via the Internet are referred to as communication enablers.
- **Network Types:** Smart environments based on IoT rely on many sorts of networks to execute collaborative activities that make people's life easier. These networks differ in supported reachability, data transfer, and terms of size.

- **Technologies:** Smart environments based on IoT use a variety of technologies to create comfortable and appropriate ecosystems.
- **Local Area Wireless Standards:** IEEE 802.15.4, IEEE 802.15.1, IEEE 802.11 are the most extensively utilised local area wireless technologies in IoT-based smart environments. These standard technologies are utilized inside the smart environment to transport data obtained from various devices.
- **Objectives:** IoT-based smart environments are being used to improve the lives of its residents in a variety of scenarios, such as elderly monitoring and assistance when travelling in the form of geo service provisioning and smart ticketing.

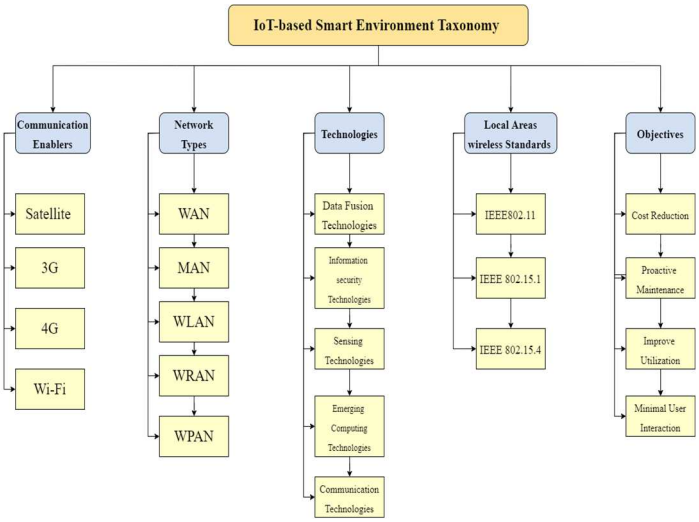

Figure 2. IoT based Smart Environment Taxonomy

IV. SECURITY THREATS AND CHALLENGES IN THE INTERNET OF THINGS (IOT)

Identification of IoT network problems and how they are dangerous, IoT devices, and IoT applications is crucial for establishing and implementing entire IoT security solutions. As below there are many Internet of Things which has security flaws identified with the Internet engineering task force.

The flows are as follows:

(a) The IoT devices cloning by untrustworthy manufacturers, (b) With malevolent lower quality items there is a substitution of lesser quality things, (c) Due to a complete lack of suitable authentication measures in place, a man-in-the-middle attack occurred during commissioning. (d) An attacker replaces the firmware with malicious code, (e) Threat to important data privacy, (f) denial-of-service (DoS) attack is a type of cyber-attack, (g) attack on the routing, (h) eavesdropping attack on IoT network that is not properly configured IoT network, and (I) extraction of security characteristics from IoT devices that are not physically unprotected. The following key IoT security concerns should be addressed in future IoT security research:

1) **Communication security:** It is crucial for the real-time movement of crucial IoT data over the Internet, as well as their safe communication. As previously stated, many IoT devices should not encrypt sensitive data before transferring it over the internet. Although secure private networking can assist to prevent vulnerabilities, it is not always the ideal option because the Internet of Things data must be exchanged and received over a large network. Packaging IoT data of a moderate quality level, such as a network of nodes, may potentially help to alleviate some of the issues. To address this problem, there are future research opportunities.
2) **Data privacy and integrity:** It's hard to protect one's privacy and honesty. Users' data should only those who have been granted permission will be able to access it. The user must grant adequate authorization before allowing others to access the data. Data must be safely disposed of when it is no longer needed.
3) **Application security:** The cloud stores data from IoT nodes, on the web, and on mobile phones. Data on a user's bank account, health, location, and other personal details could be included. Even a secure communication network will not protect the customer's data if an attacker acquires access to the data via the web, cloud, or mobile devices. As a result, safeguarding IoT data uploaded in the cloud, on the web, or on mobile devices is challenging.
4) **Vulnerability detection and management:** It's tough to discover and control numerous security risks in IoT nodes. Because there are so many of them in an IoT network, it's difficult to recognize a damaged node. More analysis is needed to design new frameworks to deal with this issue.
5) **Firmware issue:** It could be difficult to the installation of security patches and firmware updates on IoT devices. Every day, new security flaws are discovered on the internet. Users of IoT devices might have to keep track of the updates installed on their devices. All IoT devices do not support daily live updates. Users may need to unmount the device to install firmware or upgrade. To install firmware or upgrade, users may need to unmount the device. Although an automated update may be advantageous, many devices do not support over-the-air upgrades, which can cause problems.
6) **Digester recovery and incident management:** Internet of things where devices can be kept in practically any environment. And an IoT node failure might be a significant problem. As a solid digester recovery strategy and incident management are extremely restricted for real-time IoT devices, where sensitive data is handled by IoT sensors.
7) **Authentication and authorization:** IoT networks are made up of many devices. These devices must be able to join the network in a flexible manner at any moment. A significant number of devices make up IoT networks. These devices are able to join the network at any time and in a flexible manner. Without altering default passwords supplied by manufacturers, as well as using weak passwords on any gadgets, security concerns increase. Authentication and authorization are both required in this case. IoT devices have to be able to read and write to a specific database area while avoiding the rest. If the device is compromised, attackers may gain read and write access to sensitive data areas.
8) **Device identity:** IoT devices have unique identity features. Domain Name Servers give linked Internet of Things to

devices names. DNSs, on the other hand, are vulnerable to several attacks, such as man-in-the-middle attacks and DNS cache positioning attacks. DNSs, on the other hand, there are open to a variety of assaults, including man-in-the-middle and DNS cache positioning.

9) **Management of huge IoT devices:** As the number of products in IoT networks expands every day, managing them is becoming increasingly difficult. Maintaining IoT networks is becoming increasingly complicated as the number of devices in them grows by the day.
10) **Human factors:** It's difficult to deal with slacker IoT device users. For example, if a driver of a car fails to replace a defective gadget, then anyone else may be put in danger.
11) **Implementation of security algorithms:** As numerous devices in IoT networks grows by the day, managing them becomes increasingly difficult. Managing IoT networks is becoming extremely complicated as the number of devices grows by the day. Managing Internet of things networks is growing vary critical as the number of connected devices increases. As the number of linked devices grows, managing IoT networks becomes more complicated. Attackers can utilize reverse engineering to limit simple data transfer across the network. These devices' lightweight encryption techniques algorithms may help to reduce the risk of eavesdropping. structuring, installing, and testing new lightweight data security approaches in IoT networks are all research possibilities.
12) **Availability and service disruption:** IoT devices must always be able to identify and gather data. If IoT devices are hacked, physically damaged, else it can be looted, service interruption might ensue. The high accessibility of IoT devices is crucial for real-time monitoring devices.

V. Open Issues and Challenges towards the Internet of Things Based Smart Environment

Three key criteria that should be considered in any security system are availability, confidentiality, and integrity. The presence of data that can be accessed at any moment is referred to as availability. It means that no unauthorized individual has impacted the data. It indicates that the data can be accessed at any moment. Information confidentiality means that only authorized individuals have access to the data. The originality of data is ensured by integrity. Almost in every industry, every day, the Internet of things makes strides including smart agriculture, remote medical treatment, intelligent logistics, smart cities, self-driving cars, industrial monitoring, intelligent traffic management, smart GPS navigation, intelligent power networks, and smart GPS navigation, environmental management, to name a few. The integrity, availability, and security of sensitive data created by all of these smart technologies must be ensured by secure IoT solutions.

A. Open issues

Following are the open issues highlighted for future study into the Internet of things based Smart Environment considering the security challenges mentioned above:

- End-to-end IoT device identification is required for accurate authentication and authorization.
- In the IoT paradigm, there is a lot of trust between different components.
- User data generated by IoT end devices is kept private.
- IoT data security from start to end, with effective security enforcement and standardization.
- Because Intelligent Transport Systems (ITS) is part of an IoT-based smart environment, challenges are only considered for certain applications or sectors such as transportation, agriculture, healthcare, energy, and so on.

B. Issues of current Intelligent Transport Systems (ITS) architecture related to Security and Privacy

- **Excessive reliance on centralized clouds**: - Current Intelligent Transport Systems, services are Identified with the help of centralized clouds, authorize, also authenticate cars and users, as well as provide services. In such networks, cloud servers could become a bottleneck as well as a single point of failure, which causes the entire network to go down, as well as a focus for cyber-attacks and a source of private data leaks. Furthermore, as the number of linked vehicles grows, the centralized infrastructure and data storage become unscalable.
- **There is no data discrimination**: - The data that is privacy-sensitive has not been distinguished from environmental monitoring data in contemporary vehicle networks. Along with the data utilized for crowdsourcing along with services related to data are analyzed. Hence, the identities of users and vehicles are strongly linked to the data and then transferred to networks via IP addresses. This private information is maintained by service providers, among other things. Environmental data and vehicle state data, which are typically linked to customer's identities, are frequently uploaded to the cloud instead of the owner's permission. When a user uses personalized services, then the user's extensive personal information is also collected by service providers.
- **Provisioning safe and privacy-protecting services have a high overhead**: - Although current network architecture and ITS may be able to provide some secure services, the complex key management, long and complex authentication, and permission, users are hesitant to employ secure security services because of the procedures and access control procedures, as well as the expensive cost.
- **Malicious behavior is very difficult to track**: - Modern automobiles are growing increasingly reliant on onboard software and control features. An attack on a vehicle's software or control capabilities (for example, installing malicious software online) could pose a major issue that threatens the driver's and passenger's safety. Malicious behavior by service providers or other users, on the other hand, is difficult to track down and detect in a timely manner.

C. Security Issues and Challenges

The preceding section discussed the security requirements of a cloud-driven IoT-based big data ecosystem. When building an authentication strategy for such a situation, certain security needs must be taken into account. Limited computation power, scalability, dynamic security updates, protection against physical capturing, memory storage, security and privacy of IoT sensor data at the big data warehouse, energy consumption, mobility, and support for heterogeneous devices are some of the issues and challenges that have been identified. The next sections explore the

challenges and security risks involved in the IoT-based big data ecosystem powered by the cloud.

Energy requirement: There are resource-contained smart devices such as IoT sensors with limited battery backup in the given environment. When no activity needs to be reported, these devices normally aim to save energy by switching on the power saving mode. As a result of the battery backup restrictions, designing a security system that provides a high level of protection becomes extremely difficult. Hence, when creating user authentication techniques for such an environment, lightweight cryptographic procedures like the cryptograph and the AES algorithm y one-way hash function are ideal.

Protection against physical capturing: In a big data ecosystem built on IoT and the cloud, the attacker may be able to physically steal some of the smart devices like smart Sensing devices. Furthermore, an intruder can employ a power analysis attack to obtain information from an IoT sensor's memory, which can subsequently be used in other nefarious actions like calculating the user's password or computing the session key. A malicious device can be cloned and replaced by an attacker. Tamper-resistant packaging is one approach to protect against such attacks. We really should build the best strategy in such a way that if some of the smart IoT devices are stolen, the security of the communication that occurs in the remaining part of the network is not jeopardized.

Support for heterogeneous devices: We employ a variety of devices in the IoT-based cloud-based big data ecosystem, including smartphones, personal digital assistants, IoT sensors, and RFID tags. In terms of memory, power, embedded software, and computing, these devices have varying capabilities. The problem is to come up with an authentication technique that can work with a variety of devices.

Limited computation power and memory storage: In a cloud-based IoT-based big data environment, IoT devices, such as IoT sensors, have low-speed processors and limited memory capacity. In terms of performance and speed, the processing power of gadgets is limited. Furthermore, such devices are incapable of performing computationally demanding processes that necessitate a huge amount of processing power and memory capacity. As a result, developing a security solution that reduces resource consumption which means both computation and memory storage resources, while providing optimal security performance becomes difficult. As a result, we prefer to use lightweight cryptographic processes when creating user authentication algorithms for such a setting.

Security and privacy of IoT sensors data at the big data warehouse: For various types of analysis in the field, Data from IoT sensors saved in a large data warehouse can be used by the organization, estimating the probability of future fire in an industrial site, along with plausible causes. Whenever it concerns data security and privacy, such types of exposure pose significant dangers. As a result, it's critical for analysts to think about these challenges and handle data in a way that doesn't jeopardize people's privacy.

Mobility: In a cloud-based IoT-based big data ecosystem, some of the devices are mobile in nature, such as a person wearing a smart sensing device that tracks their temperature and transmits it to a cloud-based health big data warehouse. When the user is at home, these IoT devices are connected to the home network; however, when the user is away from home, they are connected to a different network, such as an office network. Different security configurations and settings are used by different networks. As a consequence, developing a security technique that is mobile-friendly is difficult.

Dynamic security updates: It is essential to maintain security schemes up to date in order to fix faults in existing schemes. e.g., Whether a new smart device is added or a device is revoked, the trusted authority will notify other network entities so that they can update their memory. As a result, building a system that allows for updates without jeopardizing or dynamic installation security is a difficult issue.

Scalability: In a cloud-based IoT-based big data ecosystem, the number of IoT devices gradually increases. Every day, most devices join the network. As a result, we usually include this capability, like the smart sensing IoT device, when building an authentication method for such an environment without jeopardizing the security requirements.

D. Future research directions and research challenges

Many research challenges and work for future towards cloud-driven IoT-based big data environment:

- Authentication across several platforms
- Heterogeneity of IoT networks environment
- Authentication scheme scalability
- Applications of data mining techniques
- Privacy-aware authentication
- The big data warehouse's data privacy is protected.
- The efficiency of using authentication schemes.
- Granular auditing
- Physically secure authentication schemes
- Security of authentication schemes

In the last, researchers can refer several applications on IoT and uses of IoTs in different sectors or its integration with other emerging technologies etc., in [16-24].

VI. CONCLUSION AND FUTURE WORK

The Internet of Things (IoT) is a multidisciplinary field in which technology and humans come together to improve people's quality of life through a better working environment and increased productivity. Numerous new technological fields are integrating with IoT for management, connection, and collaboration with the central server and gateway as the number of IoT devices grows. We've gone over twelve security issues that the IoT paradigm faces. The usage of distributed intelligence would enable instance decision making and also reduce the amount of data transferred into a cloud.

IoT security will be ensured if distributed intelligence is properly implemented on this tiered approach. Machine learning is becoming more widely used in IoT across all areas, including IoT security. Machine learning algorithms improve the IoT paradigm, but they also present new security concerns. Hacked IoT nodes can be programmed with false data by the hacker, causing it to act erratically and potentially dangerously. A trustworthy IoT infrastructure is necessary to safeguard IoT nodes against illegal access. Future IoT systems should generate a huge volume of sensitive data. Distributed intelligence, Machine learning algorithms, software-defined networking, network function virtualization, the 5G wireless network, and blockchain technologies would be used more in IoT data and networks for security, privacy, and trust in the near future. The adoption of all of these new technologies raises a number of security concerns that will require more investigation.

REFERENCES

[1] Gomez, Carles, et al. "Internet of Things for enabling smart environments: A technology-centric perspective." Journal of Ambient Intelligence and Smart Environments 11.1 (2019): 23-43.

[2] Rayes, Ammar, and Samer Salam. "Internet of things from hype to reality." Springer (2017).

[3] Stoyanova, Maria, et al. "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues." IEEE Communications Surveys & Tutorials 22.2 (2020): 1191-1221.

[4] Souri, Alireza, et al. "A systematic review of IoT communication strategies for an efficient smart environment." Transactions on Emerging Telecommunications Technologies (2019): e3736.

[5] Aufner, Peter. "The IoT security gap: a look down into the valley between threat models and their implementation." International Journal of Information Security 19.1 (2020): 3-14.

[6] Rana, Md Masud, and Rui Bo. "IoT-based cyber-physical communication architecture: Challenges and research directions." IET Cyber-Physical Systems: Theory & Applications 5.1 (2020).

[7] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." International Journal of Critical Infrastructure Protection 25 (2019): 36-49.

[8] Rao, Tariq Aziz, and E. U. Haq. "Security challenges facing IoT layers and its protective measures." International Journal of Computer Applications 179.27 (2018): 31-35.

[9] Abdullah, Amir, Harleen Kaur, and Ranjeet Biswas. "Universal Layers of IoT Architecture and Its Security Analysis." New Paradigm in Decision Science and Management. Springer, Singapore, 2020. 293-302.

[10] Stergiou, Christos, et al. "Security, privacy & efficiency of sustainable cloud computing for big data & IoT." Sustainable Computing: Informatics and Systems 19 (2018): 174-184.

[11] Ahmed, Ejaz & Yaqoob, Ibrar & Gani, Abdullah & Imran, Muhammad & Guizani, Mohsen. (2016). Internet of Things based Smart Environments: State-of-the-art, Taxonomy, and Open Research Challenges. IEEE Wireless Communications. 23. 10.1109/MWC.2016.7721736.

[12] Hajjaji, Yosra, et al. "Big data and IoT-based applications in smart environments: A systematic review." Computer Science Review 39 (2021): 100318.

[13] Kobusińska, Anna, et al. "Emerging trends, issues and challenges in Internet of Things, Big Data and cloud computing." (2018): 416-419.

[14] Fahmy, Marwa. "The Value of Big Data to the World Economy." 40.4 (2020): 307-322.

[15] Koroniotis, Nickolaos, et al. "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset." Future Generation Computer Systems 100 (2019): 779-796.

[16] Rekha G., Tyagi A.K., Anuradha N. (2020) Integration of Fog Computing and Internet of Things: An Useful Overview. In: Singh P., Kar A., Singh Y., Kolekar M., Tanwar S. (eds) Proceedings of ICRIC 2019. Lecture Notes in Electrical Engineering, vol 597. Springer, Cham. https://doi.org/10.1007/978-3-030-29407-6_8

[17] Tyagi, Amit Kumar and M, Shamila, Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices (March 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019.

[18] Reddy K.S., Agarwal K., Tyagi A.K. (2021) Beyond Things: A Systematic Study of Internet of Everything. In: Abraham A., Panda M., Pradhan S., Garcia-Hernandez L., Ma K. (eds) Innovations in Bio-Inspired Computing and Applications. IBICA 2019. Advances in Intelligent Systems and Computing, vol 1180. Springer, Cham. https://doi.org/10.1007/978-3-030-49339-4_23

[19] Tyagi A.K., Rekha G., Sreenath N. (2020) Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns. In: Satapathy S., Raju K., Shyamala K., Krishna D., Favorskaya M. (eds) Advances in Decision Sciences, Image Processing, Security and Computer Vision. ICETE 2019. Learning and Analytics in Intelligent Systems, vol 3. Springer, Cham. https://doi.org/10.1007/978-3-030-24322-7_50

[20] A. K. Tyagi and D. Goyal, "A Survey of Privacy Leakage and Security Vulnerabilities in the Internet of Things," 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 386-394, doi: 10.1109/ICCES48766.2020.9137886.

[21] Tyagi, Amit Kumar; Nair, Meghna Manoj "Internet of Everything (IoE) and Internet of Things (IoTs): Threat Analyses, Possible Opportunities for Future, Journal of Information Assurance & Security (JIAS), Vol. 15 Issue 4, 2020.

[22] Nair, Meghna Manoj; Tyagi, Amit Kumar "Privacy: History, Statistics, Policy, Laws, Preservation and Threat Analysis", Journal of Information Assurance & Security . 2021, Vol. 16 Issue 1, p24-34. 11p.

[23] Tyagi A.K., Fernandez T.F., Mishra S., Kumari S. (2021) Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, vol 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1

[24] Tyagi, Amit Kumar; Nair, Meghna Manoj; Niladhuri, Sreenath; Abraham, Ajith, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance & Security . 2020, Vol. 15 Issue 1, p1-16. 16p.