Mesopotamian journal of Cybersecurity
Vol.2023, **pp**. 85–93
DOI: https://doi.org/10.58496/MJCS/2023/013; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Review Article

An Analysis of the Internet of Everything

Roheen Qamar, [1]*, Baqar Ali Zardari [2],

[1]Department of Computer Science, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

[2]Department of Information Technology, QUEST, Nawabshah, Pakistan

ARTICLE INFO

Article History

Received 2 Feb 2023
Accepted 5 April 2023
Published 6 April 2023

Keywords
Internet Of Things
Architecture of IOT
Applications of IOT
IOT Security Services
IOT Privacy

ABSTRACT

There will be a long transition phase during which many non-PC physical objects will be connected to the Internet. This transition is known as the "Internet of Things" (IoT). However, the IoT objective cannot be achieved without computation that goes beyond the capabilities of smartphones and other handheld devices. It also has to incorporate environmental intelligence and the networking of everyday physical items. This will give rise to novel aspects of computing as well as fresh challenges. The "Internet of Things," also known as "Device communications," refers to the networking of intelligent objects of all sizes that connect with one another automatically and without human intervention. The "Internet of Things" (IoT) refers to the eventual widespread use of Internet connectivity in everyday non-computerized physical devices. However, in order to realize the IoT goal, computing must develop beyond the traditional use cases of mobile devices and smartphones to include the networking of commonplace physical things and the merging of intelligence with the surrounding ecosystem. Because of this, brand-new computer features and problems will emerge. The primary goal of this article is to examine the results of a poll on the IoT and the possible characteristics, difficulties, and privacy concerns that may occur as more and more physical goods become internet-enabled.

1. INTRODUCTION

The phrase "Internet of Things" (IoT) refers to a future in which physical things that are not typically associated with computers are linked to the Internet in some way. To make the Internet of Things a reality, computers must progress beyond the conventional mobile and smartphone apps to include networking ordinary physical things and combining intelligence with the environment. This will then result in the development of new computer functions and issues. The Internet of Things refers to the networking of smart items ranging from a little coffee machine to a massive car that speak with one another without the need for human involvement, also known as Device communications.. All technologies are growing smarter in today's developing world. Intelligent and capable of interacting with other devices Because of the heterogeneous nature of the Internet of Things, it is becoming more difficult to ensure general privacy as it rapidly expands in various domains such as smart homes, smart hospitals, and so on. There are several types of vulnerability. The phrase "internet of things" (IoT), which may be defined as numerous connected products through the internet, has acquired substantial popularity in the last decade. The Internet of Things has swiftly extended to encompass many aspects of our lives. Wearable technology, smart homes, and smart cities are a few examples. IoT devices work as intended, improving a person's quality of life with minimum effort.. As seen in Figure 1.

*Corresponding author. Email: roheen.qamar04@yahoo.com

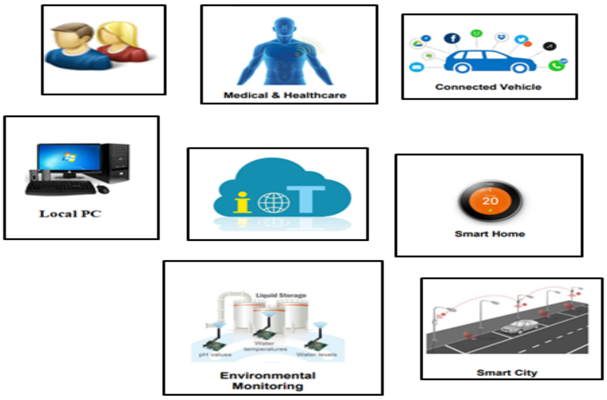

Fig.1 Internet of Things

Especially given the fact that there are no standard architecture layers for IoT (Internet of Things) applications, most research separates it into four core tiers with certain supplementary levels. The four levels are Observation, network, middleware, and applications are all components. Each layer has security flaws that make it vulnerable to various forms of assaults. We will go through IoT architecture and protocols at each tier in this post. the primary DoS/DDoS attacks, the fundamental concerns and security vulnerabilities that expose IoT to different assaults that target various IoT levels, and viable remedies and mitigation measures This revolution enables any device to connect with one another, leading to the development of a new future internet. The Internet of Things [1, 2] is a revolutionary concept for the future internet. Because of the restricted resources accessible to these devices, cyber-attacks are more focused on them. Because these devices have little computational processing memory, it is difficult to develop an efficient protection system. One of the most common IoT challenge attacks is the Hijacked Devices Conscripted into Botnets attack [3].

2. IOT ARCHITECTURE

The Internet of Things presently lacks a generally agreed architecture. Much architecture has been suggested by numerous scholars. The most basic structure, a three-layer design [4]. It was initially used at the beginning of this investigation. Perception, network, and application are its three levels

a) The Perception Layer

The perception layer is the physical layer, which contains sensors for sending and receiving environmental information. It recognizes specific physical features or locates other intelligent devices nearby.

b) The Network Layer

The network layer is in charge of connecting smart objects, network devices, and servers. Its abilities are also put to use in the transmission and processing of sensor data.

c) The Application Layer

The application layer must provide the user with access to application-specific services. Smart homes, smart cities, and smart health are just a few of the Internet of Things applications discussed. The three-layer architecture highlights the core concept of the Internet of Things, however it is not suited for IoT research because research often focuses on less significant Internet of Things characteristics. As a result, there is presently a significant growth in layered architectures in the literature. One illustration is the five-layer design [5, 6], which also contains the processing and business levels.

.

3. FUTURE VISION OF INTERNET OF THINGS

The Internet of Things is a concept that is still being developed, and depending on their usage and interests, different stakeholders may be involved in its development. Everyone is trying to understand IoT in terms of their own requirements as it is still in its infancy. The modern vision includes sensor-based data collecting, administration, processing, and the World Wide Web. Naturally, sensor-based technology is also utilized. The primary idea behind the internet of things is that there are a variety of objects or devices always present around us that are capable of connecting with one another via special addressing mechanisms, such as RFID tags, sensors, actuators, mobile phones, and so on. People help and collaborate with their neighbors to achieve a shared goal, as seen in Fig. 2 [9].

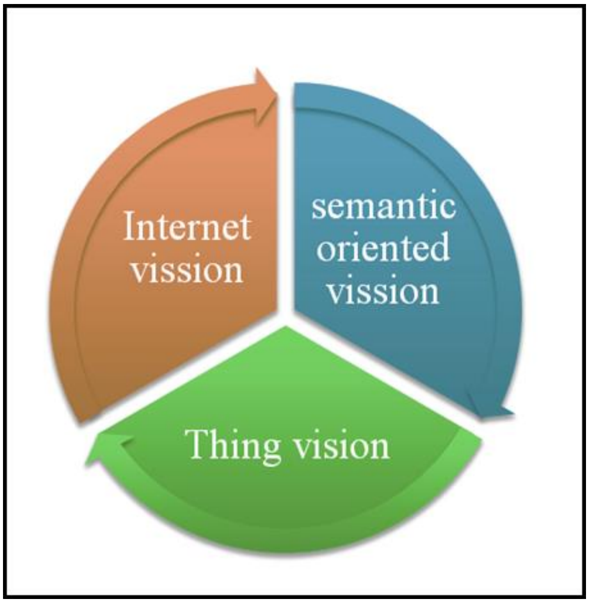

Fig 2 Future Vision of Internet of Things

They are as follows: Things Oriented Vision, Internet Oriented Vision, and Semantic Oriented Vision.

1. **Object-Oriented Vision**

The fact that we can track everything using sensors and pervasive RFID technology supports this idea [10]. To employ Electronic Product Code standards to specifically identify a product is the basic tenet (EPC). This idea is developed using sensors. It is vital to realize that in the future, vision will depend on sensors and their capacity to provide perception that is "things" oriented.

2. **Internet-Focused Vision**

The need for connected, intelligent objects has been pushed by the internet-oriented worldview. As IP is one of the primary protocols utilized in the Internet today, the objects must have IP protocol features. The sensor-based item's attributes may be continuously observed and it can be converted into a readable format with a unique identification. This provides the framework for smart embedded devices, which are designed to be little computers with processing power [11].

3. **Vision Oriented on Semantics**

Raw data must be managed, processed, and churned out in an understandable manner for better representations and understanding, and semantic technologies must be used to analyze it.

4. RELATED WORK

According to Karimi et al. [12], The Internet of Things (IoT) is a universal global neural network based on cloud technology that will facilitate communication between machines, infrastructures, environments, and things, making life safer and easier. Alsamiri, J. et al. [13] The Bot-IoT dataset was used to test various machine learning methods to identify IoT network threats, with new features outperforming the old. Jia et al. [14] In order to identify assaults in IoT contexts, an unique ML model was developed. the development of fresh DDoS defense strategies in the context of the Internet of Things, as well as Flow Guard, an edge-centric DDoS defense system. An original DDoS attack detection model and two machine learning DDoS detection and categorization algorithms are developed based on traffic variations. To demonstrate the effectiveness of the two machine learning techniques, two DDoS simulators, Slow HTTP Test and BoBeSi, each give two enormous data sets. Brun, O., Yin et al. [15] The author employed one of the most well-known deep learning approaches, the random neural network (RNN) method, in the field of Internet of Things (IoT) for identifying a DDoS assault for network detection. In compared to current methodologies, this deep learning-based methodology yields more promising findings more efficiently.

R. Vishwa karma et al. [16]. Between 2017 and 2020, the number of Internet of Things (IoT) devices is predicted to quadruple, from 8 billion to 20 billion. Many IoT devices, on the other hand, are inherently dangerous. One investigation of ten typical IoT devices found 250 weaknesses, including exposed telnet ports, outdated Linux software, and unsecured sensitive data transmission. Every day, technology advances and shrinks, bringing us closer to a "always connected" model. These botnet attacks will use infected IoT devices managed by the C&C server to launch denial-of-service (DDoS) attacks on the target host. As a result, in order to protect IoT devices and networks, an effective method for detecting this type of attack is necessary. IDS is one of the cyber-threat detection systems (intrusion detection system). DDOS attacks have escalated in recent years. DDOS attacks have expanded significantly in recent years, disrupting numerous IoT networks and inflicting major losses, for example, is a publicly accessible detecting system. Talkin Cloud et al. [17]. Due to the whole new degree of online privacy problems they provide, connected devices continue to pose serious security and privacy threats for users. This is because these gadgets may collect users' personal data, like names and phone numbers, as well as track their online activity (e.g., when users are in their houses and what they had for lunch). Customers worry about keeping too much personal data on public or private clouds for good reason.. El-hajj et al. [18] This post provides a basic, layer-by-layer overview of the security challenges and requirements in the IoT environment. The key IoT authentication systems are then reviewed using the most recent information. It analyses and investigates current authentication systems using a multi-criteria categorization as a continuation of earlier academic work, highlighting their advantages and disadvantages. Wu, Z.Q.; Zhou, et al. [19] the authors developed a framework to address IoT security issues. They used the Object Naming Service (ONS) to use an electronic product code or IP address to obtain details from the Domain Name Server (DNS) about a device (EPC). By requesting many ONSs to conceal the requester's identity, they secured the requester's anonymity. They also utilized a variety of encryption layers that communicated while utilizing the router's encryption key. Alizai, Z.A.; Tareen, et al. [20] The authors of this study proposed a Two-factor device authentication uses a digital signature and device capability to authenticate both the end-device and the server. The device decrypts the signature, solves the nonce using functional operation, signs the result, and sends it back to the server. Srinivasu, B. Vikramkumar, et al. [21] The authors presented a novel PUF-based authentication technique for IoT systems, but it is complex and lacks security analysis. Hammi, M.T.; Hammi , et al. [22] The authors suggested Vapour, a ground-breaking solution to IoT device authentication based on blockchain. The objective is to organize the devices into virtual "bubbles" where they can recognise and trust one another (concept of grouping). The communication (transaction) among various devices is then managed and verified by the Ethereum public blockchain. To offer authentication for a cloud computing system that integrates with an IoT system, Zhou, L , et al. [23] the authors presented a simple two-factor authentication technique based on XOR and one-way hashing. The three phases of the authentication procedure are password renewal, verification, and registration. Its computational cost and effectiveness in contexts with limited resources are both examined. Moghaddam, F.F. et al. [24] The authors developed an authentication technique for use in cloud computing, using an authentication server and a cloud-based Software-as-a-Service (SaaS) to authenticate registered devices. Lai, C.; Lu, R et al. [25] GLARM is a group-based lightweight authentication and key agreement scheme for resource-constrained devices. Saadeh, M.; Sleit et al. [26] The authors classify and compared a number of IoT authentication methods. The authors established two categories: the first based on the authentication approach's flatness or hierarchy, distribution or centralization, and the second based on the characteristics of the authentication procedure. Silva, E.d.O et al. [27] The authors outlined the present state of the art of authentication in an IoT setting, highlighting the obstacles and major approaches used in authentication schemes but making no comparisons.

Gebrie, M.T et al. [28] The authors gave a succinct overview of authentication methods and evaluated the systems that had been suggested in the literature. They also evaluated how much resource each approach used (e.g., energy, memory, computation and communication). Recently, Kamana et al. [29] In order to communicate and store heterogeneous IoT data related to the smart city environment, such as traffic, temperature, location, humidity, and so on, a multi-layer smart city security architecture that incorporates block chain as a distributed database layer has been developed. The data storage aims to safeguard the transfer of this data among the various smart city components. The architecture is made to deal with the dependability and scalability problems that are particularly difficult in smart city environments. Hammi, M.T. et al. [30] Bubbles-of-Trust is a revolutionary authentication solution for IoT devices based on block chain. The goal is to segregate the devices into virtual zones called bubbles where they can identify and trust one another (concept of grouping). The public block chain generated with Ethereal then manages and validates the communication (transaction) between numerous devices. Ronen et al. [31] Smart bulb attacks can be used to collect private information and create insensitive strobes, demonstrating that security issues must be considered when designing IoT devices. Hamidreza Ghorbani et al. [32] The Internet of Things (IoT) and 5G have enabled global digitalization, but when IoT and 5G come together, security challenges arise, such as the DDoS attack. Ratnaparkhi et al. [33] End-to-end security solutions are needed to ensure privacy and security of data transported through networks. Ngu, Anne H et. al. [34] Developing IoT middleware that embraces heterogeneity while retaining essential components of composition, flexibility, and security is essential for successful IoT systems. Madakam, Somayya et. al. [35] this paper provides an overview of the Internet of Things, architectures, and technologies, as well as their applicability in our daily lives. P. Suresh, J. V. et. al. [36] IoT devices can store private information, such as identify information, location information, and other personal information, which can be accessed by the public and attackers. L. Eschenauer et al. [37] highlighted research difficulties and existing solutions in the field of IoT security, concentrating on the seven major security concerns identified: authentication, access control, confidentiality, privacy, trust, secure middleware, mobile security, and policy enforcement.

5. APPLICATIONS OF IOT

The IoT's capabilities enable the development of a plethora of applications, of which only a few are being deployed. Intelligent applications for smarter homes and workplaces, smarter transit systems, smarter hospitals, smarter corporations and factories will be available in the future [38].

i. Healthcare

The Internet of Things (IoT) is being proposed as a way to improve the quality of human life by automating tasks that humans must perform. In assisted living facilities, sensors can be used to track existing prescriptions and estimate the risk of new drugs.

ii. Intelligent Water Supply

Smart cities use sensor technology to monitor water supplies and identify water loss hazards, resulting in savings of $170 million per year.

iii. Services for Smart Homes

Actuators and sensors can help reduce costs and boost energy savings by adjusting heating, cooling, and light flow to maximize energy utilization and comfort [39]

iv. Improved Fitness Centers

The gymnasium experience may be improved by incorporating new technologies such as a different exercise profile that can be loaded on equipment and each individual can be identified just by his identifying id, consequently activating the concerned profile [40].

v. Food Security

Monitoring temperature, humidity, light, and heat to protect food from climatic harm and avoid potential plant problems [40].

vi. Intelligent Parking

Smart parking provides accurate parking space information to reduce traffic congestion and CO2 emissions. [41]. this will assist to cut CO2 emissions and transportation congestion.

vii. 3D Assisted Driving

Assisted driving can provide better navigation and safety, and information about the vehicle transporting goods can be integrated to provide valuable information about delivery time, delays and faults. [41].

viii. Logistics

IoT can be used to track supply chain data, inventory, and customer happiness to reduce customer waiting time and increase sales. [41].

6. IOTS REQUIRES A WIDE RANGE OF SECURITY SERVICES

There are following various security services are necessary for IoT.

1) Data protection

Encryption/decryption is a straightforward solution to secure end-to-end communications for IoT. [42].

2) Accuracy

No intermediate should alter the core of a message as it travels from source to destination. [42]

3) Functionality

Device services must be accessible and in a continuous state to maintain availability. [42].

4) Originality

End users should be able to identify one another's identities in order to ensure that they are communicating with the same entities [42].

7. CONCLUSION

This article examines contemporary IoT research from an industrial standpoint. We begin by discussing the backdrop and service-oriented architectural models of IoT, followed by a discussion of the core technologies that may be employed in IoT. Following that, we will discuss some of the most important industrial IoT applications. Following that, we examined the research problems and future prospects related to IoT. This review paper's key contribution is that it concentrates on IoT applications and highlights the problems and potential research possibilities for future industrial researchers.

Funding

None.

Conflicts Of Interest

The authors declare no conflicts of interest.

Acknowledgment

None.

REFRENCES

[1] A. Roohi, M. Adeel, and M. Ali Shah, "DDoS in IoT: A Roadmap Towards Security & Countermeasures," in DDoS in IoT: A Roadmap towards Security & Countermeasures, 2019, no. September, pp. 5–7.

[2] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261-274, 2015.

[3] R. Vishwakarma and A. K. Jain, "A Survey Of Ddos Attacking Techniques And Defence Mechanisms In The IoT Network," Telecommunication Systems, vol. 73, no. 1, pp. 3-25, 2019.

[4] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68– 90, 2015.

[5] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.

[6] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp. 257–260, December 2012.

[7] M. Zhang, T. Yu, and G. F. Zhai, "Smart Transport System Based on 'The Internet of Things,'" Amm. 48-49 (2011) 1073–1076.

[8] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," Advances in Energy Engineering (ICAEE), pp. 69–72, 2010.

[9] M. Compton et al., "A Survey of the Semantic Specification of Sensors," in Proceedings of the 8th International Semantic Web Conference (ISWC 2009), 2nd International Workshop on Semantic Sensor Networks.

[10] D. Singh, "Developing an Architecture: Scalability, Mobility, Control, and Isolation on Future Internet Services," in Second International Conference on Advances in Computing, Communications and Informatics (ICACCI-2013), Mysore, India, August 22-25, 2013.

[11] "A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services."

[12] K. Karimi, "What the Internet of Things (IoT) needs to become a reality," 2014, Available: http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf, [Accessed 24 September, 2014]

[13] J. Alsamiri and K. Alsubhi, "Internet of Things cyber-attacks detection using machine learning," Int. J. Adv. Comput. Sci. Appl, vol. 10, no. 12, 2019.

[14] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "Flowguard: an intelligent edge defense mechanism against IoT DDoS attacks," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, 2020.

[15] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. Augusto-Gonzalez, and M. Ramos, "Deep learning with dense random neural networks for detecting attacks against iot-connected home environments," in International ISCIS Security Workshop, Springer, Cham, 2018, pp. 79-89.

[16] R. Vishwakarma and A. K. Jain, "A Survey Of Ddos Attacking Techniques And Defence Mechanisms In The IoT Network," Telecommunication Systems, vol. 73, no. 1, pp. 3-25, 2019.

[17] "IoT Past And Present: The History Of Iot, And Where It's Headed Today," Talkin Cloud, 2016. [Online]. Available: http://talkincloud.com/cloud-computing/iot-past-andpresent-history-iot-and-where-its-headed-today?page=2. [Accessed: 27-Jul-2023].

[18] [18] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," in Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 2017, pp. 1–3.

[19] Z. Q. Wu, Y. W. Zhou, and J. F. Ma, "A Security Transmission Model for Internet of Things," Chin. J. Comput., vol. 34, pp. 1351–1364, 2011.

[20] Z. A. Alizai, N. F. Tareen, and I. Jadoon, "Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures," in Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 2018, pp. 1–5.

[21] B. Srinivasu, P. Vikramkumar, A. Chattopadhyay, and K. Y. Lam, "CoLPUF: A Novel Configurable LFSR-based PUF," in Proceedings of the 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 2018, pp. 358–361.

[22] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computer. Secur., vol. 78, pp. 126–142, 2018.

[23] L. Zhou, X. Li, K. H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," Future Gen. Comput. Syst., vol. 91, pp. 244–251, 2019.

[24] F. F. Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, N. M. Alibeigi, and S. D. Varnosfaderani, "A scalable and efficient user authentication scheme for cloud computing environments," in Proceedings of the 2014 IEEE REGION 10 SYMPOSIUM, Kuala Lumpur, Malaysia, 2014, pp. 1–4.

[25] C. Lai, R. Lu, D. Zheng, H. Li, and X. S. Shen, "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications," Comput. Netw., vol. 99, pp. 66–81, 2016.

[26] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication Techniques for the Internet of Things: A Survey," in Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2016, pp. 102–108.

[27] E. d. O. Silva, W. T. S. de Lima, F. S. Ferraz, and F. I. do Nascimento Ribeiro, "Authentication and the Internet of Things: A Survey Based on a Systematic Mapping," in Proceedings of the Twelfth International Conference on Software Engineering Advances, Athens, Greece, 2017, pp. 20-25.

[28] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for Internet of things in smart home eHealth," in Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, Canterbury, UK, 2017, pp. 102–108.

[29] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016, pp. 1392–1393.

[30] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computer. Secur., vol. 78, pp. 126–142, 2018.

[31] E. Ronen and A. Shamir, "Extended functionality attacks on iot devices: The case of smart lights," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P), March 2016, pp. 3–12.

[32] H. Ghorbani, M. S. Mohammadzadeh, and M. H. Ahmadzadegan, "DDoS Attacks on the IoT Network with the Emergence of 5G," in 2020 International Conference on Technology and Entrepreneurship-Virtual (ICTE-V), 2020, pp. 1-5.

[33] S. Ratnaparkhi and A. Bhangee, "Protecting Against Distributed Denial of Service Attacks and its Classification: An Network Security Issue," IJCSI International Journal of Computer Science Issues, vol. 3, no. 1, 2013.

[34] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: A survey on issues and enabling technologies," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1-20, 2016.

[35] S. Madakam, V. Lake, and V. Lake, "Internet of Things (IoT): A literature review," Journal of Computer and Communications, vol. 3, no. 05, pp. 164-173, 2015.

[36] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, 2014, pp. 1-8.

[37] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security, ser. CCS ’02, 2002, pp. 41–47.

[38] "Internet of Things –A Future of Internet: A Survey," International Journal of Advance Research in Computer Science and Management Studies Research Article / Paper / Case Study Available online at: www.ijarcsms.com.

[39] "4th international conference on modern circuits and system technologies: A survey of IoT: Architecture, Applications and Future Vision."

[40] R. Parashar, A. Khan, and A. K. Neha, "A survey: The internet of things," International Journal of Technical Research and Applications, vol. 4, no. 3, pp. 251-257, 2016.

[41] "Big Data on Internet of Things: Applications, Architecture, Technologies, Techniques and Future Directions," International Journal of Computer Science Engineering (IJCSE).

[42] Z. Ren, X. Liu, R. Ye, and T. Zhang, "Security and privacy on internet of things," in 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 2017, pp. 140-144.