Recent Advances of Security in IoT: A Survey

Anita Adhikari[a], Rishab Sharma[a] and Akalanka Mailewa[b]

[a]Department of Information Systems, St. Cloud State University, St. Cloud, MN, United States

[b]Department of Computer Science and Information Technology, St. Cloud State University, St. Cloud, MN, United States

Abstract

The internet of things is performing a very crucial role holding capability to connect devices with the storage. This system is based on a multilayered architecture of IoT which has four components perception, network, middleware, and application layers that help in building a secure system. IoT has helped in the development of new technology that suggests certain techniques for security. This also helps in using WSN as well as RFID for data collection and processing. The change in technology and services has convenient impact on people's life. This paper helps to understand the different layers of IOT, security issues as well as security in IoT with the use of different techniques. Some of the technologies such as blockchain system, intrusion detection in machine learning, advancement in 4G/5G networks related to IoT devices are addressed.

Keywords: IoT, Risk, Vulnerabilities, Security, Wireless Sensor Networks, RFID, Attacks

1. Introduction

This era is completely dependent on new things as well as evolving technology which has helped every individual to learn about advanced techniques and methods of performing the task smoothly and precisely. The Internet of Things is widely used expression which was first used in the year 1999 by Kevin Ashton, a British technology Pioneer who defined IoT as the system of physical objects in the world that connects to the internet through a sensor [l], [2], [3], [4], [5]. The main working function of IoT is to interact with other machines, objects, environments as well as infrastructures and other related aspects that help to create a new idea to perform any task. This helps to establish communication to the digital world with the help of internet through the collective network of connected physical devices such as sensors, actuators, and controllers and so on. The current technology relating to IoT includes some concepts such as Wireless Sensors Networks (WSN), Machine-to-Machine(M2M) communicating system, or other technology as RFID (Radio- frequency Identification) [6]. IoT consists of various areas including cloud, mobile devices, virtualized environments, sensors, Radio Frequency Identification (RFID), and Artificial Intelligence that works for maintaining secure system [7]. There is chance of increment in user holding high probability in future with increment of security issues and challenges because any people with bad intension can attack on these devices through the connection of internet access. The security of the Internet of Things has been a point of concern because of its analysis through the environment in which thoughts are emerging to another generation in which billions of devices are connected only through the internet. Some kinds of security issues are vulnerabilities, malware that hamper the entire security of the system [8].

2. Working functionality of IoT

As the system is emerging every moment, things need to be up to date and functional for which there should be a working procedure for each task. In a similar way, IoT system holds four different components with certain property that give better result of performance of the system. Those components are sensors/devices, connectivity, data processing and user interface holding an important role to conduct the whole IoT working system. All these components are related to the working procedure of the IoT which is shown in the figure below. At first, the sources are studied for data collection process and computation is implemented by sensors for any kind of change occurred on the system. Sensors play a very important role in any kind of smart application by detecting any physical/chemical change and after processing the collected data they automate the services to make it intelligent or ready to use. There are different types of sensors such as proximity, position, occupancy etc. that help to establish communication with other devices and nodes without human intervention [9]. The new data is collected from the environment along with useful information with the help of sensors. Those data are converged with the environment for the comparison with some aspects. After that, those collected data needs to be analyzed and then connection can be established to the cloud from the environment from which data are retrieved. Connectivity is the source of communication that helps to establish connection between data and cloud with the help of some connecting resources like cellular data, Wi-Fi, etc. When connection is established, the data processing helps to proceed those data which is done by the system, this consist of different protocols that's needs to be followed to obtain accuracy in results. After this, the user interface plays an important role for interaction with computer system [10].

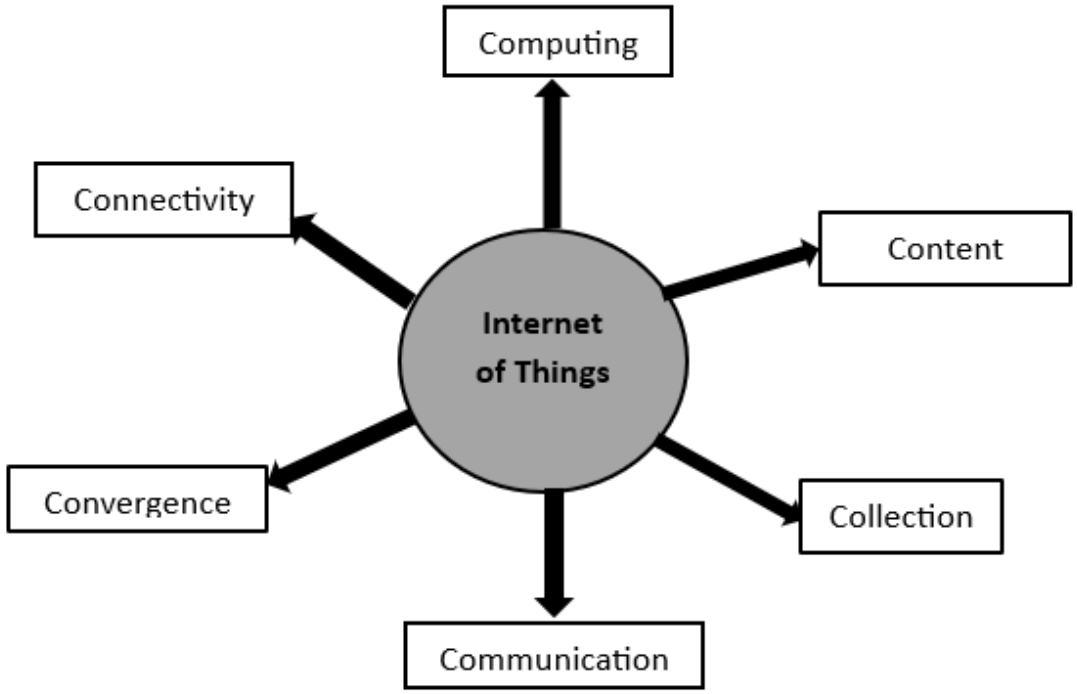

Figure-1 Working mechanism related to components of Internet of Things [11]

3. Security Requirements in IoT

A network connected physical device that isn't a computer is considered an IoT device. Since most IT professionals are focused on protecting standard IT devices with traditional network security, protocols and technologies, the security risks and threats associated with the Internet of things and their devices are less well known. In short, IoT security is an underdressed problem in many organizations all over the world. The traditional cybersecurity systems are not developed regarding IoT security, hence standard IT security systems created in the past like IDPs (Intrusion Detection/Prevention system), and firewalls are not capable of recognizing internet of things devices or the unique risk profiles associated with it. For instance, IoT devices are deployed by business sectors. All network connected devices such as printers, cameras, sensors, lighting, scanners have their own hardware, chipsets, firmware that introduce their own vulnerabilities and risks. These vulnerabilities may bypass typical cybersecurity controls and processes. Which is why it is important for enterprises and the IT industry to address the vulnerabilities and threats associated with IoT systems [12].

However, the data security and privacy concerns might only be at one end of the spectrum. The potential risks associated with IoT may reach new levels such as interoperability, autonomous decision-making etc. might create complexity and create more vulnerabilities related to that service in the long run. On the Internet of things, a lot of information is related to personal information such as Name, DOB, registration, IP addresses, budgets, and lots more [13]. For instance, IoT is becoming very popular in the health industry with remote monitoring of patients with cardiac pacemakers by helping doctors receive data over long distances and different places in real time. The systems transfer critical information like temperature and ECG through Wi-Fi or GSM technology depending on the IoT system in practice. This vital information, if fell into the wrong hands might create life threatening circumstances [14].

This is just one aspect of a challenging problem and cybersecurity professionals will need to ensure that they think through the potential privacy and risks associated with the entire data set. The Internet of Things should be implemented in an ethical, lawful socially and politically acceptable way with the consideration of legal, systematic, economic, and technical implications. The main research challenges in the IoT sector include confidentiality of data, its privacy, and integrity that impact on the system.

For the better understanding of the IoT security requirements, a four layered architecture is introduced. The four layers include: perception layer, network layers, middleware layer and application layer. Each of the layers provides corresponding security controls such as authentication, integrity, availability and access control during the transmission and storage of data.

4. IoT Framework for Assessment Measures & Policies

The loT system architecture consists of multiple layers showing up its own functionality such as sensing, communicating, processing the data and information that provides security to the whole model. The data transmission process is performed with various sources from which they are extracted and modified via network connection. The system must hold a high secured environment to perform all the functions so that the chance of data loss is comparatively less. In this paper, we have discussed about four-layer architecture that consists of Perception Layer, Network Layer, Middleware Layer and Application Layer that work together to make system functionality better. The Perception Layer helps in data collection process whereas Network layer helps in data transmission process over the network [15]. The data is processed after receiving by Middleware Layer and those data can be accessed by user with the help of Application Layer. This data can be used by the user for making plans and policies for performing certain tasks in Business layer [1][16][17]. In figure-2 the four-layered architecture is reflected below.

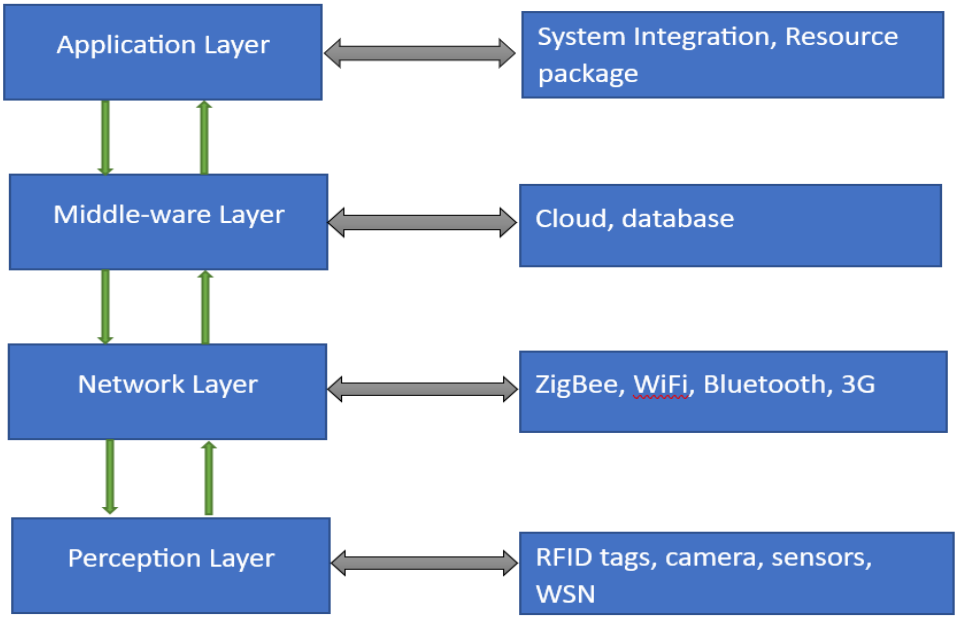

Figure-3: loT four-layered architecture [17]

A. Perception layer

Perception layer is also defined as the Sensor layer or device layer that helps in data collection process. First, the raw data and information are collected from different sources and then it examines the working environment under which the data is transferred from one point to another. The main factors that help to make perception layer understandable are minimization of cost, deployment, communication process and so on. It is considered as the actual hardware of the loT system that consists of sensor-enabled physical objects where connected devices are real endpoints. The main functions of this layer are sensing, actuating monitoring, communicating as well as controlling the environment under which the task is performed. Some sensors are RFID tags, barcodes, QR code, camera, WSN etc. which works under the requirements of application to gather information regarding surroundings such as location, time, user details as well as other factors [18]. After the information is gathered, they are converted into digital signals and passed to the network layer. The data collection seems to be an easy task but there are some security issues for this process. The source of data needs to be authorized ones so that there is less chance of attacks on the system.

B. Network Layer

The network layer is commonly called connectivity layer or edge-computing layer that receives data from the perception layer and transfers it from sensor devices to the data processing units. For transferring data through the internet, wired or wireless modem can be used. For maintaining connection between different components there should be verification of the actual data source that means the connection needs to be more secure. The technologies like ZigBee, Wi-Fi, Bluetooth, 3G etc. with some protocols like 1Pv4, IPv6, MQTT, DDS etc. can be used according to the nature of sensor devices so that data can be distributed and processed at the edge of network [19]. The loT communication protocols are divided into sensor-based network and gateway-based network by some of the research related activity which ensure whether the communication is secured or not [20]. Most of the basic communication protocols are used in this layer to ensure the connection between objects. Some of the security related issues in network layer are network management technologies, efficiency of energy related to network and requirements related to quality of services that should be address and managed for enabling devices to give better performance. Once the connection is established the data is transferred to the Middleware layer for processing efficiently.

C. Middleware Layer

Middleware Layer receives the data from the network layer and stores it in the database to prevent data loss. For the analysis of those data, some data analytics can be used which can help in service management because IoT devices are implemented for serving services related to technology. Communication can be established only between those smart objects which come under similar types of service. The function of this layer is data processing, computation, cloud computing and automatic decision making based on the type of results that ensures direct access to the database to store all the information. The data received can be analyzed with advanced data analytics because this layer is mostly compatible with the cloud infrastructures as integrated with the cloud services. In other words, big data storage along with high computing applications can be placed at this layer [21]. There can be chance of some security issues such as storage of same data multiple times, lack of computation and so on. The data can be stored separately according to its characteristics to arrange in a systematic manner and avoid duplication.

D. Application Layer

This layer holds an interface which establishes interconnection with the entire IoT system which can be small tracking to the whole system that works under certain protocols. Similarly, a variety of things are managed by an IoT system which notifies the user about the conditions and results are created based on those data. The data needs to be represented by those applications which also control and monitor the IoT systems. The IoT application front end part is known as an application layer that is accessible to the user. The applications implemented by IoT can be a smart home, smart city [22], smart healthcare, smart farming, smart retail, and intelligent supply chain [23] that is managed by application layer depending on data processed by middleware layer.

5. Security Issues in IoT

IoT security at both the physical devices and service applications are critical for its success. Various problems and loopholes remain in every step of the way such as security and privacy protection, network protocols, standardization, identity management, trusted architectures and so on.

As the standard cybersecurity measures are developed and practiced with little regard to IoT security, the systems have an expanded attack surface. On top of this, insecure practices among users who may or may not have the resources or knowledge to protect their IoT systems makes the condition worse. Some of the well-known issues in IoT include the following [8]:

- **Vulnerabilities**: We know that no system is safe because there will always be zero-day attacks or vulnerabilities. However, one of the main reasons IoT devices are vulnerable is because of the insufficient computational power and capacity for security. The reason behind this could be the limited budget available for the development, testing and production of secure firmware for the devices. The lack of budget not only affects the hardware components but the web applications and related software which may lead to compromised systems.
- **Malware**: However, limited the capacity of the systems, hackers still find a way to infect malware into the devices. IoT botnets related malware are one of the recent and most prevalent cases, as they are economic and versatile for cybercriminals. In the recent advent and popularity of crypto currency, IoT hackers have been found mining crypto currency and spreading ransom ware through botnets.
- **Escalated cybercrimes**: IoT devices are used as botnets which infect more machines while masking their malicious actions. Smart home botnets have seen a surprising number of unforeseen attacks in the year 2020.
- **Information theft and exploitation**: As mentioned in this report, connected devices and transmission of data over the network increases the attack surface and chances of exposure online.

6. Future Directions with ongoing Research or Advancement

The main goal is to ensure a complete secure IoT system with the use of the applications which holds multiple issues and challenges. There are mainly two factors for ensuring the security of the IoT that impacts on the system. The first factor is maintaining a standard architecture to ensure secure communication in perception layer in the context of internet. Whereas second factor is the selection of suitable algorithm for encryption for the fulfillment of IoT devices capacity with the analysis of energy consumption as well as processing capacity. This section describes some future direction which will help to enable secure IoT.

A. Introducing Standardized Algorithms

The researchers are making efforts to build a secure encryption algorithm which is kind of easy to use in daily activities. The main reason behind issues for building such algorithm is limited capacity of IoT devices in terms of power consumption, memory capacity and processing features. There should be declaration for the minimum requirement of such algorithms in terms of key size, consumption of energy and time taken to perform tasks so that the devices can be recognized as per their ability. Some kind of conventional algorithms have been used to secure the IoT which provide lower memory use in context of both hardware and software [24]. Not only this, But AES has also been derived to provide secure communication between the IoT devices [25].

B. Use of machine learning for security

For better security to IoT devices, there has been increased interest in the use of machine learning these days [26]. Some machine learning algorithms are introduced to extract data from network traffic for the analysis of unauthorized users. Several attacks like Distributed Denial of Service (DDoS) attacks are increasing rapidly against IoT networks with certain techniques such as botnets [27]. For the analysis of such attacks, certain analysis detection mechanisms are introduced that determine the detailed information of the source of attacks and help in finding solution that prevent the system. Machine learning is also used for intrusion detection systems that match characteristics of IoT that requires real time monitoring [28].

C. Blockchain in Smart loT

Blockchain is the distributed ledger that is secure, transparent, and immutable which can be used to create decentralized database for storing information as per the requirement [29]. It can be used in many application fields such as supply chain management, industries, network virtualization working together in a distributed decentralized network to add more security features in case of handling large amount of data and information. But this algorithm cannot be implemented in those IoT devices with limited resources and mobile edge server because of high energy consumption and computing capacity. There are several advanced applications in IoT devices which can implement block chain mechanisms that help to enhance spectral efficiency and provide much better optimization with secure privacy policy [30]. Although there are a lot of advantages that block chain offers but there is no specific framework that can provide a complete secure solution to meet the confidentiality, integrity, and availability triad to preserve the privacy.

D. Securing 4G/5G and beyond application

There is various taxonomy of attacks against 4G/5G cellular networks presented that affect privacy, availability, integrity, and authentications [31]. Although there are various countermeasures provided for the preservation of privacy based on cryptography methods, human factors, intrusion detection system to fulfill the requirements related to security of IoT in context of 5G, there should be more research implemented to achieve the targeted goal of making them more secure and precise [32][33]. There are some kinds of security related issues that need to be resolved such as absence of dataset, location, and identity privacy based on 5G scenarios. There is some recent research going on like capacity extension of massive channels using waveforms to improve the performance of 5G mobile networks which can increase the number of connected IoT devices [34][35].

7. Conclusion

On the positive side, the Internet assists rn detection, monitoring, and transmission of important data without the need of human interaction. It certainly has made day-to-day life easy for individuals as well as business enterprises and processes. IoT devices have also been used for healthcare and road safety by incorporating different kinds of sensors that sense potential dangers and notify the individual or authorities if necessary. On the other hand, the complexity of IoT systems and the lack of focus on IoT security, there can be many vulnerabilities in the IoT systems. Intruders may access vital information and it could even be life threatening in the wrong hands. In this paper, we discussed the security requirements and potential threats in the four-layer architecture. We mainly focused on the 4-layer architecture and the connection between them with regards to general device security, network security, communication security and application security. We reviewed the security challenges in the existing and upcoming Internet of things systems and services as well. The implementation of security measures such as blockchain, intrusion detection system, machine learning is most important to perform for achieving the required system in the application area. Although the system is derived, there should be more research to fulfill the advancement in security of IoT related devices.

References

[1] Khan, Saad, and Akalanka B. Mailewa. "Discover Botnets in IoT Sensor Networks: A Lightweight Deep Learning Framework with Hybrid Self-Organizing Maps." Microprocessors and Microsystems (2023): 104753. (DOI: https://doi.org/10.1016/j.micpro.2022.104753).

[2] N. Damayanti, "Internet of Things : a v1s10n, architectural elements, and future directons," Internet of Things a vzszon, architectural elements, and future directons, May 2016, Accessed: Feb. 01, 2023. [Online]. Available: http://edocs.ilkom.unsri.ac.id/194/

[3] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," Wireless Personal Communications, vol. 58, no. 1, pp. 49-69, Apr. 2011, doi: 10.1007/s11277-011-0288-5.

[4] T. V. Narayana Rao, S. K. Saheb, and A. J. Ram Reddy, "Design of Architecture for Efficient Integration of Internet of Things and Cloud Computing," International Journal of Advanced Research in Computer Science, vol. 8, no. 3, pp. 392-396, Mar. 2017, Accessed: Feb. 01, 2023. [Online]. Available: https://web.s.ebscohost.com/ehost/detail/detail?vid =0&sid=718dcb15-339b-4cc0-a05c- 1338fl ca2abc%40redis&bdata=JnNpdGU9ZWhvc 3QtbG12ZSZzY29wZTl zaXRl#AN=122961254&d b=aci

[5] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of Things: Evolution, Concerns and Security Challenges," Sensors, vol. 21, no. 5, p. 1809, Mar. 2021, doi: 10.3390/s21051809.

[6] C. Mahmoud and S. Aouag, "Security for Internet of Things," Proceedings of the 9th International Conference on Information Systems and Technologies, Mar. 2019, doi: 10.l1 45/3361570.3361622.

[7] 0. Edewede, D. Jazani, and G. Epiphaniou, "Internet of Things Forensics: Challenges and approaches", In: Proc. of 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), IEEE, 2013. Available Online: DOI: 10.4108/icst.collaboratecom.2013.254159

[8] TrendMicro, "IoT Security Issues, Threats, and Defenses Security News," www.trendmicro.com, Jul. 22, 2021.https://www.trendmicro.com/vinfo/us/security/new s/inte rnet-of-things /iot-sec urity-101-threats-issues- and-defenses

[9] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M. Rahmani, and P. Liljeberg, "On the Feasibility of Attribute-Based Encryption on Internet of Things Devices", IEEE Micro, Vol. 36, No. 6, 2016, pp. 25-35. Available Online: http://doi.org/l 0.1109/MM.2016.101

[10] Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL based medical data processing and retrieval: the exposome project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. 2017.

[11] J. Amalraj, S. Banumathi, and J. John, "IOT Sensors And Applications: A Survey." [Online]. Available: https://www.i js tr.org/final-print/aug2019/Iot-Sensors-And-Applications-A- Survey.pdf

[12] "What Is loT Security?," Palo Alto Networks. https://www.paloaltonetworks.co m/cyberpedia/wha t-is-iot-security

[13] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," Internet Research, vol. 26, no. 2, pp. 337-359, Apr. 2016, Accessed: Feb. 04, 2023. [Online]. Available: https://nrl.northumbria.ac. uk/id/eprint/26551/?fbcli d=IwAR0z2aNgBYzKzIC8cGK2zlvtF7d4zQz6T7 K9O lkiGSKcgl 6uMRriwFZlGNE

[14] Abdul-jabbar, Hassnaa & Abed, Jameel. (2020). Real Time Pacemaker Patient Monitoring System Based on Internet of Things. IOP Conference Series: Materials Science and Engineering. 745. 012093. 10.1088/1757- 899X/745/1/012093.

[15] V. S. Narwane, R. D. Raut, B. B. Gardas, M. S. Kavre & B. E. Narkhede, "Factors affecting the adoption of cloud of things: The case study of Indian small and medium enterperises", Journal of Systems and Information Technology, 21(4), 397- 418, 2019.

[16] Singh, Nicholas, Kevin Bui, and Akalanka Mailewa. "Robust Efficiency Evaluation of NextCloud and GoogleCloud." Advances in Technology (2021): 536-545. (DOI:10.31357/ait.v1i2.5392)

[17] K. Chen et al., "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," Journal of Hardware and Systems Security, vol. 2, no. 2, pp. 97-110, May 2018, doi: 10.1007/s41635-017-0029-7.

[18] A. Khan, M. H. Rehmani, & A. Rachedi, "Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions", IEEE wireless communications, 24(3), 17-25, 2017.

[19] Ying Zhang, "Technology Framework of the Internet of Things and Its Application," in Electrical and Control Engineering (ICECE), 2011, pp. 4109-4112

[20] P. P. Ray, "A survey on Internet of Things architectures," Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 3, pp. 291-319, Jul. 2018, doi: 10.1016 /j.jksuci.2016.10.003.

[21] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig, & S. Sanguanpong, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks" IEEE access, 7, 107678-107694,2019.

[22] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran & S. Guizani, "Internet-of- things-based smart cities: Recent advances and challenges", IEEE Communications Magazine, 55(9), 16-24, 2017.

[23] D. Miorandi, S. Sicari, F. De Pellegrini, & I. Chlamtac, "Internet of things: Vision, applications and research challenges", Ad Hoc Networks, 10(7), 1497-1516, 2012.

[24] S. Rajesh, V. Paul, V. Menon, and M. Khosravi, "A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices," Symmetry, vol. 11, no. 2, p. 293, Feb. 2019, doi: 10.3390 /syml 1020293.

[25] W. Yu and S. Kose, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 64, no. 11, pp. 2934-2944, Nov. 2017, doi: 10.1109/tcsi.2017.2702098.

[26] Khan, Shehram Sikander, and Akalanka Bandara Mailewa. "Detecting Network Transmission Anomalies using Autoencoders-SVM Neural Network on Multi-class NSL-KDD Dataset." In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0835-0843. IEEE, 2023.

[27] A. Carlin, M. Hammoudeh, and 0 . Aldabbas, "Defence for Distributed Denial of Service Attacks in Cloud Computing," Procedia Computer Science, vol. 73, pp. 490-497, 2015, doi: 10.1016/j.procs.2015.12.037.

[28] Jairu, Pankaj, and Akalanka B. Mailewa. "Network Anomaly Uncovering on CICIDS-2017 Dataset: A Supervised Artificial Intelligence Approach." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 606-615. IEEE, May 2022. (DOI:10.1109/eIT53891.2022.9814045)

[29] Ndri, Anna, Divya Bellamkonda, and Akalanka B. Mailewa. "Applications of Block-Chain Technologies to Enhance the Security of Intrusion Detection/Prevention Systems: A Review." In Midwest Instruction and Computing Symposium (MICS), vol. 2, p. 4. 2022.

[30] E. H. H. Kure, P. Engelstad, S. Maharjan, S. Gjessing, and Y. Zhang, "Distributed Uplink Offloading for IoT in 5G Heterogeneous Networks Under Private Information Constraints," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6151- 6164, Aug. 2019, doi: 10.l109/JIOT.2018.2886703.

[31] H. Mrabet, "Performance Investigation of New Waveforms in CRAN Architecture for 5G Communication Systems," IEEE Xplore, Mar. 01, 2020 .https://ieeexplore. ieee.org/abstract/document/ 9096676 (accessed Feb. 04, 2023).

[32] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities." Cluster Computing 23 (2020): 1955-1971.

[33] Mailewa, Akalanka, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Mechanisms and techniques to enhance the security of big data analytic framework with mongodb and Linux containers." Array 15 (2022): 100236. (DOI:10.1016/j.array.2022.100236).

[34] Moore, Tristan L., Samuel S. Conlon, Anushka U. Hewarathna, and Akalanka B. Mailewa. "Encryption Methods and Key Management Services for Secure Cloud Computing: A Review."

[35] Johnson, Chapin A., Sharveen Paramiswaran, and Akalanka B. Mailewa. "Discovering Vulnerabilities in Web Browser Extensions Contained by Google Chrome."