Literature Review on IoT-based Cyber Security Attack detection technique for Smart City

Mrs. Yogita Pralhad Shewale, (Research Scholar SJJTU-Reg No: 29821048)

yogitashewalenet.shewale@gmail.com

Dr. Shailesh Kumar, shaileshkumar1610@gmail.com (Computer Science and Engineering, Associate Professor in Gopalan College of Engineering Management, Bangalore.

Dr. Banait Satish Shankarro, Email: ssbanait@kkwagh.edu.in (Computer Department of K.K. Wagh Institute of Engineering and Research Center, Nashik.

Abstract—The Internet of Things (IoT) is rapidly growing, now a day's very fast , in Industry 4.0, environmental monitoring, home automation, smart mobility, and. personal health care for that so many devices deployed in various of sectors of public and private environments usefull for making society task easy and automated IoT now a days in lot of demand in such a scenario, cyber security becomes important part which can't be avoid or exploit because the sensible information, denial of service (DoS) attacks, unauthorized network access, and so on. Unfortunately, IoT not support to strong security mechanisms, The aim of this survey is to provide a broad overview of the security risks and attacks in section of IoT security and preventions measures after a general introduction to security in the IoT domain to this end, discuss the perticular security mechanisms adopted by the most popular IoT research papers. Then, to report and analyze some of the attacks against real IoT devices reported in. we gives the details of security measures that utilized in most of IoT base research areas again analyze some device reported some of IoT attacks in real environment . Afterword analyze the weaknesses of IoT solutions in cyber security finding Anomalies and about Security Attributes and access limitations to provide access control, authorization and authentication by many of the researchers regarding the IoT -base cyber security domain.

Index Terms—Attacks, devices, Internet of Things (IoT).

I. INTRODUCTION

Internet of Things (IoT) paradigm is now is now a day's very popular in each domain and increasing the popularity in simplifying the everyday takes by remotely by monitor environments, vehicles, and buildings, and so on connecting people by everyday object through the sensors and actuators. [1]. From last few years IoT devices have grown rapidly last years, with a prediction of over 50 billion devices connected to the Internet by 2020 [2]. The IoT devices are quickly spreading in all environments, like New “smart” services , such as smart appliances, smart houses, smart watches, smart TVs becoming everyday more pervasive. Moreover, many of such smart services require users to intentionally reveal some personal (and, sometimes, private) information in change for advanced and more personalized services. As per the analysis it's found that security is having importance if inadequate, incomplete, or ill-designed security mechanisms. IoT growing fast interaction from last few decades to transmit sensitive

II. LITERATURE REVIEW

Ozcelik et al. [1] have developed an edge-oriented detection & mitigation strategy employing software-defined networking (SDN) and fog methods to combat DDoS in IoT. SDN was used as a flexible method to lay up the fresh flow rules and dynamically update them as necessary. This proposed method showed that it is possible to mitigate DDoS attacks for IoT devices using SDN. to the hardware itself using edge computing. A lightweight, deep-packet anomaly detection method was developed by Summerville et al.[2] for use with IoT devices that have limited power computing prowess. The n-gram bit patterns used in this work include used and it is permitted for the n-gram size to vary by dimension.

Pa et. Al.[3] suggested an IoT honeypot to collect data and sandbox to examine attacks that use Telnet that is launched from a large number of IoT devices using various CPUs. The Analysis reveals that the DDOS malware files that were recovered are from a minimum of five distinct families a brief light on game theory. The proposed anomaly detection system in [4] is capable of running on

DOI : 10.35291/2454-9150.2022.0501

hardware with constrained processing power.An anomaly and specification were proposed by Bostani et al. [5].Who used based intrusion detection system for recognizing 2 routing incidents referred to as sinkhole and selective forwarding incidents in IoT.

The larger literature tends to concentrate on several broad key themes related to smart cities, such as the privacy and security of mobile devices and services, smart cities' technical architecture, power systems used within smart cities, smart healthcare, security and privacy frameworks, algorithms and protocols, operational threats for smart cities, application of blockchain solutions within smart cities, and social media and smart cities.

The research themes and the proportion of papers categorized under each category are shown in Figure 1. Table 1 contains a list of the themes and relevant sources. The article's subsections stimulated conversation around each theme, including details on the study done under each of the primary themes.

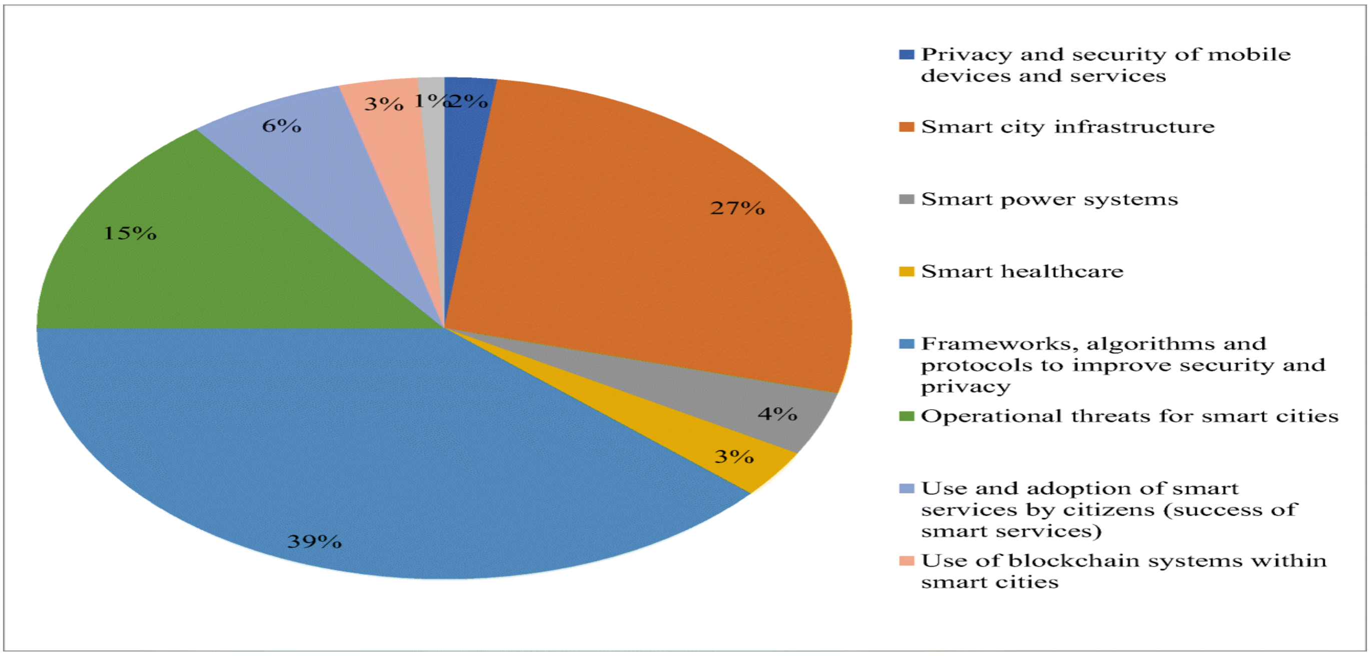

Fig 1. Security, Privacy, and Risks Within Smart Cities

Evolutionary self-cooperative mechanisms have been proposed by Ruo Jun Cai et al. (2020) as a defense against malicious nodes. By computing, a node can recognize the maliciousnode.the worth of trust. To improve its accuracy, theproposed system makes use of a joint strategy to identifycriminal nodes It is a protocol based on records. The strategybased on past performance forecasts the trust. itself the assessment process mostly relies on the records kept atadjacent nodes. Each node can calculate the trustbased on the information obtained. The collaborative strategy isdynamic in actuality. The shares of the trust are obtained from computing a single value leveraging the trust between various nodes.portions [28].

In general, the relevance of intrusion detection in securing networks has drawn the attention of numerous researchers. Numerous published publications offer solutions or methodologies for intrusion detection in wireless sensor networks & IoT applications. A neural network-based intrusion detection system has recently been developed by Batiha et al. [30], with a particular emphasis on how the learning process affects classification accuracy & energy usage.

Sekhar et al. [31] created an IDS method based on deep Autoencoder and Fruitfly optimization. When dealing with missing data in the datasets, they used fuzzy C-Means. After that, they used a deep autoencoder to extract robust features, which they then fed into a back propagation neural network to categorize attacks. Additionally, the Fruitfly algorithm was used to optimize the Autoencoder's hidden layers. The evaluation revealed that the suggested strategy worked effectively using data from the NSL-KDD and UNSW-NB15 datasets.

TCP SYN network assaults were explored by B. K. Mohanta, U. Satapathy, and D. Jena, [32], and J. Li and B. Sun [33] developed deep neural networks for attack detection in IoT systems. Risk assessment was carried out, the system was mapped, and the self-adaptive identification method of the security index of the network was explored.

Table 1 contains a list of the themes and relevant sources.

Theme	References
Mobile device and service privacy and security	Li et al. (2019)[12]. ; Abi Sen et al (2018)[13].
Infrastructure for smart cities	Antoine Picon (2019)[14]. ; Awad et al. (2019)[15]. ; Bernardes et al. (2018)[16].
Intelligent power systems	Ainane et al. (2018)[17].; Alamaniotis et al. (2017)[18].
Threats to smart cities' operations	Grieman (2019)[19].; Habibzadeh et al. (2018)[20].; Kitchin and Dodge (2019)[21].;
Citizen use and acceptance of smart services (success of smart services)	Babdullah et al. (2017)[22]. ; Chatterjee et al. (2018)[23].
Using blockchain technology in smart city applications	Mora et al. (2019)[23].; Noh and Kwon (2019)[24].; Ramos and Silva (2019)[25].
Smart cities and social media	Moustaka et al. (2019)[26].

Reference	Application	Performance
Aubert and Pahl. (2018) [6].	Using simply the communication between services in distributed multi-dimensional IoT microservices in an IoT site, a machine learning-based technique can predict IoT service behavior.	This approach has a 96.5 percent overall accuracy for anomaly identification and a 0.2 percent false positive rate.
Chilamkurti and Diro. (2018) [7].	Employing the NSL-KDD to compare the effectiveness of a deep model and a shallow neural network, researchers developed a deep learning model to detect widespread threats in an unsocial IoT network.	In addition to 95.22 and 96.75 percent accuracy, their model also obtained 99.2 and 98.27 percent accuracy.
Pajouh et al. (2016) [8].	They discovered low-frequency attacks such as user-to-root (U2R) and remote-to-local (R2L) assaults from the NSL-KDD dataset and suggested a two-stage dimension reduction & classification technique to detect abnormality in IoT backbone networks.	attained an identification rate of 84.82 percent.
Kozik et al. (2016) [9].	Developed an attack detection method that made use of the Apache Spark cloud architecture's extreme learning machine (ELM)technology. The Netflow-formatted data that are gathered from the fog computing environment can be efficiently computed and analyzed thanks to the ELM architecture and features. This research focused on three key IoT system use cases: scanning, command and control, and infected hosts.	99 percent, 76 percent, and 95 percent accuracy levels.
Isakov & Kinsy. (2019) [10].	Created and applied a \ secure and robust technique for supporting sensitive\information-sharing in IoT.	attained an identification rate of 90.82 percent.
Groninger & Ghosh. (2021)[11].	Have provided a data analytics review using edge cloud computing for the Internet of Things. Here, the Edge cloud's embedded intelligence technique is carried out using the Deep Learning methodology. SDN-focused adaptable strategy for combating SC applications SEAL strikes are DoS assaults.	Sliding windows can reduce data on the edge by up to 80% without significantly reducing accuracy when they are employed in the preparation stage.
Hui Zhang et al. (2020) [29].	for an IoT-based Smart city context, have introduced safe data management design. The three layers of the proposed system include data security. layer, a layer for calculation, and a layer for decision-making. The data security layer now includes an encryption technique. for maintaining the data's integrity. Utilizing a payload-based Scheme for symmetric key encryption.	According to simulation studies, evolutionary self-cooperative trust (ESCT) increases network scalability and assures successful routing in mobile ad hoc networks (MANETs) even while attackers are causing routing interruption.
Zagrouba R, Alhajri R. (2021) [34].	The deductive technique was applied in this study's execution, and known data and tests were run and investigated to provide accurate data and conclusions that are made. These deductions were made using various materials. on machine learning, particularly in the IoT space. Our claimwill begin by concentrating on general theories and concepts, then putting these ideas to use in practical applications	accuracy rating of greater than 99.99%, with a true positive rate of 1 and a false negative rate of 0.
Gill HS, Singh T, Kaur B, Gaba GS, Masud M, Baz M. (2021) [35].	The goal of this research project is to protect huge multimedia data from cyber abuses by incorporating artificial intelligence and machine learning.	The outcomes demonstrate the security of the frame encryption approach, and the proposed scheme is appropriate for use with multimedia systems, Internet communication, and secure communications.
AbuAlghanam O, Qatawneh M, Almobaideen W, Saadeh M. (2022) [36].	To facilitate the provision of smart city applications, a new hierarchical key distribution (HKD) architecture and a collection of hierarchical hybrid key distribution (H2KD) protocols are given. The HKD architecture has been used to study the applicability of these protocols, and Burrows-Abadi-Needham (BAN) logic and the AVISPA tool were	The analysis's findings demonstrate that the H2KD saves constraint nodes 51.5 percent in communication, compute, and storage expenses when compared to similar protocols.

DOI : 10.35291/2454-9150.2022.0501

	both used in the simulation.	
Ajaeiya et al. (2022)[37].	proposed for IDS that solely makes use of network functionality and is anomaly-based. With a 99.5 percent true positive rate and a 0.001 percent false positive rate, the R-tree approach surpasses the other machine learning models.	Their findings demonstrated the potency of mathematical techniques like Random Forest. On the other hand, their dataset is not a test that prompts concerns about its validity.
Reddy KR, Satwika C, Jaffino G, Singh MK. (2023) [38].	The smart monitoring system described in this manuscript relies on wireless technology. This technique gathered real-time data on an urban setting using Zigbee.	This document describes the conception & development of the Zigbee for smart cities, as well as how to use it.
Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. (2022) [39].	This evaluation's objective is to ascertain the CNN model's result. The suggested deep learning model was tested using experiments on benchmark datasets that were made available to the public. The models' performance and accuracy were assessed using the accepted measures.	To increase the performance and security of the IoT network, this research provided a model based on convolutional neural networks (CNN).
Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, Abdulkadir SJ. (2022) [40].	We propose a systematic literature review (SLR) of the literature on AI techniques for detecting cybersecurity intrusions in the IoT context, which maps, classifies, and surveys the literature.	This investigation also sheds light on the AI roadmap for identifying dangers depending on the types of attacks. We conclude by offering suggestions for potential new investigations.
Reddy DK, Behera HS. (2022) [41].	On the DS2OS dataset, many researchers' previous methods are examined and briefly discussed using the suggested technique.	To perform intelligent & adaptive anomaly detection for smart home environment devices, the CatBoosting approach was presented in this research. The suggested method helps to better manage resources while monitoring the data for both normal and anomalous activity.
Rajasoundaran S, Prabu AV, Routray S, Malla PP, Kumar GS, Mukherjee A, (2022) [42].	Each sensor node is protected by the dynamic multi-watchdog system that is proposed on Deep Learning (DL) by keeping track of node transmission. The proposed study also includes secure node- and data-centric evaluation techniques, which are necessary for extending the secure medium of 5G-based IoT-WSN networks.	The performance of suggested cooperative multi-watchdog system performs 10% and 15% better than previous methods.

III. REFERENCES

[1] M. Ozcelik, N. Chalabianloo, and G. Gur, “Software-Defined Edge Defense Against IoT-Based DDoS,” in 2017 IEEE International Conference on Computer and Information Technology (CIT). IEEE, 8 2017, pp. 308–313.

[2] D. H. Summerville, K. M. Zach, and Y. Chen, “Ultra-lightweight deep packet anomaly detection for Internet of Things devices,” in 2015 IEEE 34th International Performance Computing and Communications Conference, IPCCC 2015, 2016.

[3] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoTPOT: A Novel Honeypot for Revealing Current IoT Threats,” Journal of Information Processing, vol. 24, no. 3, pp. 522–533, 2016.

[4] H. Sedjelmaci, S. M. Santucci, and M. Al-Bahri, “A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology,” in 2016 IEEE International Conference on Communications (ICC). IEEE, 5 2016, pp. 1–6.

[5] H. Bostani and M. Sheikhan, “Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach,” Computer Communications, 2017.

[6] Pahl, M.O.; Aubet, F.X. All eyes on you: Distributed Multi-Dimensional IoT microservice anomaly detection.In Proceedings of the 2018 14th International Conference on Network and Service Management (CNSM),Rome, Italy, 5–9 November 2018; pp. 72–80

[7] Dior, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener. Comput. Syst. 2018,82, 761–768.

[8] Pajouh, H.H.; Javidan, R.; Khatami, R.; Ali, D.; Choo, K.K.R. A two-layer dimension reduction and two-tierclassification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans. Emerg.Topics Comput. 2016,7, 314–323.

[9] Kozik, R.; Chora´s, M.; Ficco, M.; Palmieri, F. A scalable distributed machine learning approach for attack detection in edge computing environments. J. Parallel Distrib. Comput. 2018,119, 18–26.

[10] Bu, L., Isakov, M. & Kinsy, M. A. (2019). A secure and robust scheme for sharing confidential information in IoT systems, Ad Hoc Networks, 92, 101762. DOI: 10.1016/j.adhoc.2018.09.007

[11] Ghosh, A. M. & Grolinger, K. (2021). EdgeCloud Computing for Internet of Things Data Analytics: Embedding Intelligence in the Edge with Deep Learning, IEEE Transactions on Industrial Informatics, 17(3), 2191-2200.

[12] Abi Sen, A. A., Eassa, F. A., & Jambi, K. (2018). Preserving privacy of smart cities based on fog computing https://doi.org/10.1007/978-3-319-94180-6_18.

[13] Li, J., Zhang, W., Dabra, V., Choo, K., -., R., Kumari, S., & Hogrefe, D. (2019). AEP-PPA: An anonymous, efficient, and provably-secure privacy-preserving authentication protocol for mobile services in smart cities. Journal of Network and Computer Applications, 134, 52–61. https://doi.org/10.1016/j.jnca.2019.02.003.

[14] Antoine Picon, G. (2019). Smart cities, privacy, and the pulverization/reconstruction of individuals. European Data Protection Law Review, 5(2), 154–155. https://doi.org/10.21552/edpl/2019/2/4.

[15] Awad, A. I., Furnell, S., Hassan, A. M., & Tryfonas, T. (2019). Special issue on the security of IoT-enabled infrastructures in smart

cities. Ad Hoc Networks, 92. https://doi.org/10.1016/j.adhoc.2019.02.007.

[16]. Bernardes, M. B., De Andrade, F. P., & Novais, P. (2018). Smart cities, data, and right to privacy: A look from the Portuguese and Brazilian experience. Paper presented at the ACM International Conference Proceeding Series, 328–337. https://doi.org/10.1145/3209415.3209451.

[17] Alandjani, G. (2018). Features and potential security challenges for IoT-enabled devices in a smart city environment. International Journal of Advanced Computer Science and Applications, 9(8), 231–238.

[18] Aldairi, A., & Tawalbeh, L. (2017). Cyber security attacks on smart cities and associated mobile technologies. Paper presented at the Procedia Computer Science, 109, 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391.

[19] Gupta, P., Chauhan, S., & Jaiswal, M. P. (2019a). Classification of smart city research-a descriptive literature review and future research agenda. Information Systems Frontiers, 21(3), 661–685.

[20] Habibzadeh, H., Soyata, T., Kantarci, B., Boukerche, A., & Kaptan, C. (2018). Sensing, communication, and security planes: A new challenge for a smart city system design. Computer Networks, 144, 163–200. https://doi.org/10.1016/j.comnet.2018.08.001.

[21] Krawiec, R. J., Barr, D., Killmeyer, J., Filipova, M., Nesbitt, A., Israel, A., Quarre, F., Fedosova, K., & Tsai, L. (2016) "Blockchain: Opportunities for health care," CP Transaction. Available at: https://www.colleaga.org/sites/default/files/4-37-hhs_blockchain_challenge_deloitte_consulting_llp.pdf. Accessed on 28 March 2020.

[22] Babdullah, A., Rana, N. P., Ali, A. A., Dwivedi, Y. K., & Lal, B. (2017). Assessing Consumer's Intention to Adopt Mobile Internet Services in the Kingdom of Saudi Arabia. AMCIS 2017, Boston, USA, 10-12th August 2017.

[23] Chatterjee, S., Kar, A. K., & Gupta, M. P. (2018). Alignment of IT authority and citizens of proposed smart cities in India: System security and privacy perspective. Global Journal of Flexible Systems Management, 19(1), 95–107. https://doi.org/10.1007/s40171-017-0173-5.

[24] Mora, O. B., Rivera, R., Larios, V. M., Beltran-Ramirez, J. R., Maciel, R., & Ochoa, A. (2019). A use case in cybersecurity based on blockchain to deal with the security and privacy of citizens and smart cities' cyberinfrastructures. Paper presented at the 2018 IEEE International Smart Cities Conference, ISC2 2018, https://doi.org/10.1109/ISC2.2018.8656694.

[25] Noh, J., & Kwon, H. (2019). A study on smart city security policy based on blockchain in 5G age. Paper presented at the 2019 International Conference on Platform Technology and Service, PlatCon 2019 - Proceedings, https://doi.org/10.1109/PlatCon.2019.8669406.

[26] Ramos, L. F. M., & Silva, J. M. C. (2019). Privacy and data protection concerns regarding the use of blockchains in smart cities. Paper presented at the ACM International Conference Proceeding Series, Part F148155 342–347. https://doi.org/10.1145/3326365.3326410.

[27] Moustaka, V., Theodosiou, Z., Vakali, A., Kounoudes, A., & Anthopoulos, L. G. (2019). Enhancing social networking in smart cities: Privacy and security borderlines. Technological Forecasting and Social Change, 142, 285–300. https://doi.org/10.1016/j.techfore.2018.10.026.

[28]H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon and X. Li,"SafeCity: Toward Safe and Secured Data Management Design forIoT-Enabled Smart City Planning," in IEEE Access, vol. 8, pp.145256-145267, 2020, DOI: 10.1109/ACCESS.2020.3014622.

[29] R. J. Cai, X. J. Li, and P. H. J. Chong, "An Evolutionary SelfCooperative Trust Scheme Against Routing Disruptions inMANETs," in IEEE Transactions on Mobile Computing, vol. 18, no.1, pp. 42-55, 1 Jan. 2019, DOI: 10.1109/TMC.2018.2828814.

[30] Batiha T., Krömer P.Design and analysis of efficient neural intrusion detection for wireless sensor networksConcurr. Comput.: Pract. Exper., 33 (23) (2021), Article e6152

[31] Sekhar R., Sasirekha K., Raja P., Thangavel K.A novel GPU-based intrusion detection system using deep autoencoder with fruitfly optimizationSN Applied Sciences, 3 (6).

[32] J. Li and B. Sun, "A Network Attack Detection Method Using SDA and Deep Neural Network Basedon Internetof Things," International Journal of Wireless Information Networks, vol. 27, no. 2, pp. 209–214, Jun. 2020, https://doi.org/10.1007/s10776-019-00462-7.

[33] N. Sahar, R.Mishra, and S. Kalam, "Deep Learning Approach-Based Network Intrusion Detection System for Fog-Assisted IoT," in Proceedings of International Conference on Big Data, Machine Learning and their Applications, Singapore, 2021, pp. 39–50, https://doi.org/10.1007/978-981-15-8377-3_4.

[34] Zagreb R, Alhajri R. Machine Learning based Attacks Detection and Countermeasures in IoT. International Journal of Communication Networks and Information Security. 2021 Aug 1;13(2):158-67.

[35] Gill HS, Singh T, Kaur B, Gaba GS, Masud M, Baz M. A metaheuristic approach to secure multimedia big data for IoT-based smart city applications. Wireless Communications and Mobile Computing. 2021 Oct 4;2021.

[36] AbuAlghanam O, Qatawneh M, Almobaideen W, Saadeh M. A new hierarchical architecture and protocol for key distribution in the context of IoT-based smart cities. Journal of Information Security and Applications. 2022 Jun 1;67:103173.

[37] Saba T, Khan AR, Sadad T, Hong SP. Securing the IoT System of Smart City against Cyber Threats Using Deep Learning. Discrete Dynamics in Nature and Society. 2022 Jun 26;2022.

[38] Reddy KR, Satwika C, Jaffino G, Singh MK. Monitoring of Infrastructure andDevelopment for Smart Cities Supported by IoT Method. In Proceedings of Second International Conference in Mechanical and Energy Technology 2023 (pp. 21-28). Springer, Singapore.

[39] Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering. 2022 Apr 1;99:107810

[40] Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, Abdulkadir SJ. Detecting Cybersecurity Attacks in the Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics. 2022 Jan 10;11(2):198.

[41] Reddy DK, Behera HS. boosting Approach for Anomaly Detection in IoT-Based Smart Home Environment. In Computational Intelligence in Data Mining 2022 (pp. 753-764). Springer, Singapore.

[42] Rajasoundaran S, Prabu AV, Routray S, Malla PP, Kumar GS, Mukherjee A, Qi Y. Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks. Computer Communications. 2022 Apr 1;187:71-82.