IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 2, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

Review on Quantum Security Model for IoT based Smart Environment

Iteesh Goel[1], Chandra Mohan B[2].

UG Student, SCOPE, VIT Vellore, India[1]

Associate Professor (Senior), SCOPE, VIT Vellore, India[2]

ABSTRACT: The Internet of Things (IoT) is a broad phrase that describes the billions of physical objects or "things" that are connected to the Internet and are all capable of collecting and exchanging data with other systems and devices. The Internet of Things (IoT) is a new approach to infrastructure organization that uses affordable, portable devices that can manage everyday chores and optimize operations across a huge infrastructure. The Internet of Things has made it possible for the physical and digital worlds to interact and collaborate. By enabling firms to automate and streamline their regular processes, it provides them with a host of advantages.In this survey, we have examined some of the research papers and made a summary about securing the IoT devices in smart environments using different techniques mentioned in there methodologies. Through this survey we can make up the use of the different techniques present in the environment to avoid the cyberattacks in the IoT devices to avoid leaking of confidential data. They examined blockchain method to securing sending the data towards different receivers by using hash functions which lead to high security towards data encryption. Also they have examined some of the ML training models which lead to securing the data at a very high extent.

KEYWORDS: IoT, Smart Network, Quantum Cryptography, Cyber Security.

I. INTRODUCTION

One of the current technology innovations with the quickest rate of development is the Internet of Things (IoT). However, growing security worries about things like software flaws and hackers may discourage many users from utilizing IoT devices. These IoT security issues are particularly important for businesses operating in the healthcare, finance, manufacturing, logistics, retail, and other sectors that have already begun implementing IoT devices. In this post, they discuss the definition of IoT security, its importance, and the main threats it is vulnerable to. They also go over how to secure networks, devices, and data in IoT environments.

The Internet of Things (IoT) is now in its early stages, but it will eventually have an impact on practically all of the everyday products we use. By converting previously offline systems into online ones, IoT will very soon widen the scope of cyberattacks on homes and companies. Existing security technologies are just insufficient to address this issue. Blockchain has come to light as a potential remedy for future IoT system security issues.Securing IoT devices is a complex and challenging task, as these devices are often vulnerable to cyber attacks due to their limited processing power and memory. Some of the key issues in securing IoT devices include:

(a) Identity management and authentication.
(b) Data security.
(c) Security of the network.
(d) Security for software and firmware.

Blockchain technology has the ability to solve a number of problems with IoT device security. One of the main advantages of using blockchain is its capacity to offer safe and decentralized identity management and authentication for IoT devices. Without the requirement for a centralized authority, blockchain enables IoT devices to have a distinct and unchangeable identity that can be independently validated by other IoT devices on the network. Only approved devices will be able to connect with one another, preventing unauthorized access to the network.Quantum cryptography tools and services may prove to be quite beneficial in this area. Furthermore, by using cutting-edge quantum computing and communication technologies, dangers connected with cloud storage and data transfer that are frequently linked to blockchain and IoT might be significantly reduced or even eliminated. Originally intended to be the quantum equivalent of random walks, quantum walks are a crucial tool for algorithm development.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

II. REVIEW ON PROTECTING SMART ENVIRONMENTS IN IOT: EXAMINING THE VIABILITY OF QUANTUM SECURITY SOLUTIONS

Internet of Things (IoT) systems' security and privacy have come under scrutiny as a result of the growing use of IoT devices in smart environments including homes, offices, and cities. As Internet of Things (IoT) devices proliferate and become more linked, they become more susceptible to cyberattacks, which may jeopardize sensitive data and interrupt essential services. Researchers are looking into novel security solutions based on quantum technologies as a response to these problems.

1.1. ATTACK DETECTION IN DISTRIBUTED SMART APPLICATIONS.

The Internet of Things (IoT) is a new method of organizing domestic automatons and infrastructure using inexpensive, portable devices that can manage routine tasks and optimize operations over a large infrastructure[1]. While there are unquestionably many benefits to using IoT, there are also significant difficulties related to object security that must be addressed in order to maintain services. Ad hoc solutions can be built on a wide variety of architectures and platforms, starting with single-board microcontroller units (MCUs) like Arduino and STM32 and ending with single-board portable computers like Raspberry Pi, Cubieboard, Orange Pi, etc[2].The IoT system is vulnerable to several types of cyberattacks, as the Mirai botnet attack showed, while advanced data analytics and machine learning have demonstrated effectiveness in a variety of cybersecurity applications, such technologies have not yet been sufficiently investigated in the literature from the standpoint of their applicability in the domain of resource-constrained IoT[3]. According to F-secure, a security company, cyberattacks on IoT devices are growing quickly; in 2019, more than 2.9 billion attack events involving IoT devices were reported[4].

In this contribution, they demonstrate how an Artificial Neural Network model for identifying clever similarity-based network assaults may be trained and used to simple IoT nodes. In order to strengthen the cybersecurity on microcontrollers, this paper puts forth the idea of a resource-constrained intelligent system as a component of the Internet of Things (IoT) infrastructure[5].

This paper has double contribution. It first shows how data analytics may be used to defend IoT end-node devices from cyberattacks. Second, it outline a framework for an intelligent system that could be implemented in the IoT ecosystem to help the detection of network assaults, which would entail IoT end-nodes being actively involved (in contrary to more powerful IoT gateways).

(a)Methodology: Distributed ML-Aided cyberattacks Detection on IoT Nodes.

The research of the use of ML for cybersecurity in the IoT ecosystem, namely network threat detection, is covered in this section. As a matter of fact, we assess the applicability and computational burden that the most popular ML model, ANN, can add to actual IoT applications. They have decided to focus on the most universal components for the review phase, as they are currently in use by the public and are well-maintained.

(b) Use Case and Suggested Model.

This contribution's objective is to provide a method and launch a demonstration of how advanced data analytics can be employed in part on IoT nodes as well as IoT gateways. IoT nodes and IoT gateways typically connect to the primary data storage via custom network lines or Internet connections. I suggest utilizing an advanced data analytics strategy based on clever IoT infrastructure components. In this ML model they have taken the improvised dataset- NSL-KDD. An ANN is trained in two stages. If using a sigmoid activation function, the output calculation step and weights update step will be as follows.

$$y_{actual} = sigmoid[(x_1 \cdot w_1 + \cdots + x_N \cdot w_N + b) - \theta]$$

$$w^i_{new} = w^i_{old} + \alpha \cdot (y_{target} - y_{actual}) \cdot x_i$$

(c) Testing-Attack detection phase.

The network packet that is received is compared to the trained model during the testing phase. Intrusion Prevention Systems (IPS) systems and IDS/IPS systems are similar in that they inspect network traffic and compare it to predefined signatures.

This study investigates the present state of the art in terms of IoT end-node device security measures, the applicability of Machine Learning, and existing data analysis standards. In addition to the standard cybersecurity measures for IoT gateways, they suggest a notion of the intelligent model training for IoT end-node device-based network assaults

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

detection. In addition, a proof-of-concept implementation using an Arduino Uno Rev3 MCU with 2 KiloByte RAM shows how Artificial Neural Networks can be used for accurate and intelligent network attack detection. It is evident that using the chosen features, the model can be trained to classify previously unknown network data even on an IoT end-node in about 2 ms while requiring 16 training epochs to attain the required accuracy.

2.2: DECISION-MAKING MODEL.

A new category of industrial initiative known as the "industrial Internet of Things" (IIoT) offers a greater level of production flexibility in terms of product specification, quality, resource usage, and cost-efficiency[6]. In order to provide production flexibility in terms of resource and cost utilization, the IIoT is a network-centric paradigm. Devices develop new functional capacities to extract knowledge from facts and develop plans based on them as a result of implementing these notions. Classical intelligent systems focused on the comfort of human living and energy conservation and were primarily concerned with monitoring and adjusting the environment within specified predefined ranges.

In this paper, they offer a paradigm for making decisions regarding the security of IIoT data. Using the Technique for Order Preference by Similarity to the[7]. Ideal Solution, can transmit and store information securely while employing a variety of communication parameters. A safe detection system that can identify malicious devices and take informed actions, such as stopping their activity, is required to stop these problems[9]. Intelligent Management Systems (IMS) are crucial for connecting production and applying big data analysis to give information for decision-making. An effective smart system that senses and manages its immediate surroundings in accordance with the information gathered from various sources is proposed in order to develop a trusted decision-making model to control and handle communicated information. Simple additive weighting (SAW) and Technique for Order Precedence by Similarity to the Ideal Solutions (TOPSIS) approaches are hierarchically combined with intelligent systems to produce an effective and precise decision-making process[10].Numerous measurement factors, including message alteration, record accuracy, trusted devices, detection rate, and denial-of-service (DoS) threats, are used to thoroughly examine the performance of the proposed model.

To maintain safe network connection, it is essential to identify authentic devices. The suggested mechanism effectively filters out malicious devices, as opposed to baseline approaches that mistakenly list more malicious nodes as trusted nodes. They can observe that using various criteria helps to identify trusted nodes more accurately.As more IoT devices are added, the baseline technique performs poorer and becomes less effective. The security systems must be able to distinguish between legal devices and malicious ones since the number of IoT devices is growing along with it. The suggested method effectively distinguishes between malicious and trusted nodes. Existing techniques, however, are unable to reliably discern between them and locate trusted nodes in the network.

When more IoT devices are added to the system, the rate of data tampering grows, but more slowly than in the current schemes due to the involvement of malicious nodes.

This is because trusted IoT devices may be efficiently identified by employing a variety of measurement parameter approaches. It is challenging for an attacker to hack any IoT device due to the use of many criteria because the system can quickly identify any rogue nodes.The cause of the proposed method's superior performance to the baselinetechnique combines the SAW method with TOPSIS to filter out BAs while calculating each node's trust and to guarantee the accuracy of the records.

2.3: SECURING IOT DATA USING BLOCKCHAIN.

The Internet of Things (IoT) is now in its early stages, but it will eventually have an impact on practically all of the everyday products we use. By converting previously offline systems into online ones, IoT will very soon widen the scope of cyberattacks on homes and companies[11]. Existing security technologies are just insufficient to address this issue. Blockchain has come to light as a potential remedy for future IoT system security issues. This paper first provides an overview of blockchain technology and how it is implemented. Next, they examine the IoT infrastructure, which is based on the blockchain network, and finally, a model for the security of the internet of things using blockchain is offered[12]. Consensus, which offers proof of work (PoW) and checks network activity is the first pillar of blockchain technology[13]. The second pillar is ledger, which provides comprehensive information about network transactions[14].

In this article, a method is provided on using blockchain technology, in this post to create a more secure network, trustworthy IoT model. They came to the conclusion that the internet of things would not be a full participant in a

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

blockchain network due to the high-end hardware requirements. However, the functions added by blockchain technology through the APIs provided by network nodes or by other specialized intermediaries would undoubtedly benefit the internet of things. These features could make the internet of things extremely safe. They have talked about the cybersecurity aspect of the brand-new and developing blockchain technology. Since Bitcoin is a cryptocurrency that is built on blockchain technology, research in this area is primarily focused on and uses blockchain technology. However, they attempt to include blockchain technology in our essay for the internet of things to provide secure data transfer between internet-connected devices. For this, they have provided an overview of blockchain technology, discussed and proposed blockchain as a solution for IoT Security, and provided information on security concerns in the IoT context.

2.4: QUANTUM BASED CYBERSECURITY.

The creation of protocols and technology that would enable us to create more responsive, dynamic, and engaging cities in order to enhance daily life is the core goal of the notion of smart cities, which has evolved in recent years. It is important to emphasize that the development of smart cities requires not only the building of high-tech infrastructure and services, but also the involvement of citizens in the provision and improvement of services[17]. Numerous studies and experience reports have suggested that the transition to smart cities should be carried out gradually in order to assure success and sustainability as well as by tackling the most important issues that have an impact on people' daily life. Smart city advantages coexist with new potential hazards[18].Investment is necessary on both the technical and social fronts, particularly in the key areas of networking and communication infrastructures, data collection and analysis, social and crowdsourcing technologies, policies and regulations, and information security, to implement efficient smart utilities[19].

Quantum cryptography tools and services may prove to be quite beneficial in this area[20]. Furthermore, by using cutting-edge quantum computing and communication technologies, dangers connected with cloud storage and data transfer that are frequently linked to blockchain and IoT might be significantly reduced or even eliminated.
In cybersecurity, blockchain is essential[18]. The majority of present cryptography techniques may be broken with the efforts made to realize large-scale quantum computers. Therefore, a quantum tool used to develop blockchain frameworks must be able to execute at the level of digital computers and fend off attacks that could come from any or both of these types of computers[21]. Here, they provide a novel authentication and encryption technique based on quantum walks (QIQW).

A blockchain's units each have a hash value that links them to both the prior and subsequent blocks. They use QHF with public key parameters to construct the hash value that connects each block in the chain to the one before it in our suggested blockchain design. Our approach presupposes that each stakeholder on the blockchain system has a validated profile and its own key settings for each node in the system in order to limit illegal or destructive access to the network.
Initialization: Public key parameters are shared between all stakeholders in order to run QHF for joining blocks of the chain.

Key exchange: Key parameters for intended nodes are exchanged by each stakeholder node over quantum secure channels or in a closed environment.
Encryption: Data is encrypted by the sender using the key settings of the intended node. Sender ID, receiver ID, cypher contents, and the transaction's timestamp make up each transaction.
Verification: The blockchain system alerts the receiver node that a new transaction needs to be confirmed, and the receiver then uses its own parameters relating to the intended sender to run the decryption algorithm to decode the data.
Linking: The running block is increased with each successful transaction. Then, QHF is used with public key parameters to connect the most recent block to its predecessor in the chain. The system's nodes then add this new block to their respective blockchains.

In this research, they introduced a novel QHF-based cybersecurity protocol created by quantum-inspired quantum walks. The proposed protocol used to construct a quantum-inspired blockchain for the safe transfer of data among IoT devices for smart water utilities took into account the necessity for privacy and secrecy in IoT devices for smart water utilities. Additionally, they used QHFs for connecting the current block to the chain's previous block. Our suggested protocol can fight against message attacks and man-in-the-middle attacks, according to the security study, guaranteeing safe data transmission between IoT devices. The fundamental benefit of our research is that it provides a framework for developing blockchain solutions that can withstand potential attacks from both digital and quantum computers.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

2.5: MACHINE LEARNING BASED IOT SECURITY.

The network of internet-connected electronic items, such as sensors, smartphones, and wearables, is referred to as the "Internet of Things" . In addition to giving consumers more convenience and control, these gadgets also frequently offer effective solutions to end-user industries including manufacturing, automotive, and healthcare[22]. The market is expected to grow due to the increase in cloud platform adoption, development of wireless networking technologies, emergence of advanced data analytics, and a reduction in the cost of connected devices[23]. In these applications, data security is of utmost importance. The data's availability, confidentiality, and integrity must all be guaranteed. Without adequate protection, cyber-attackers might simply enter the local IoT network, read or alter the data gathered, and/or conduct a DoS attack that would prohibit authorized users from using the application or viewing the data[24]. Devastating outcomes from a cyber-attack can include significant financial losses, data breaches, fines and regulatory penalties, a loss of consumer and stakeholder trust, and operational disruptions.

Machine learning (ML)-based intrusion detection algorithms can be a useful defense against attacks in IoT systems[25]. In this study, they have suggested an intrusion detection methodology that uses big data and machine learning (ML) to identify infiltration in IoT networks. In order to train models for attack categorization and anomaly detection in IoT networks security, they created and assessed a software framework employing a Hadoop cluster to store large datasets[26].

This study employed a large IoT dataset and machine learning techniques to identify IoT network assaults. Because of its frequent updates, extensive attack diversity, and range of network protocols, the Bot IoT dataset was chosen. They selected useful characteristics for attack classification and anomaly detection using Random Forest feature selection. Our suggested methodology includes the processing and training of models utilizing a Hadoop-Spark cluster, which is a distributed storage and computation framework, as they hoped to exploit the vast dataset to produce a more generic model. The suggested methodology shows how the Hadoop-Spark cluster can be used to analyze big data and train an IoT intrusion detection machine learning model using a large dataset. In terms of reconnaissance attack detection, both ADM and MCM deliver satisfactory results with the highest accuracy of 99.9%. The intrusion detection system does not need labelled data for anomaly detection, which is another benefit of the proposed framework.

III. RESULTS AND DISCUSSION

The paper 1 examines the state-of-the-art in terms of data analytics standards, machine learning's application, and security measures for IoT end-node devices. In addition to the usual IoT gateway cybersecurity precautions, they suggested an intelligent model training for IoT end-node device-based network assaults detection. In paper 2,the suggested model classifies critical parameters utilizing the TOPSIS technique for its decision-making model with the IIoT.

The suggested approach uses the TOPSIS method to identify valid IoT devices so that the CM can recognize accurate sensing reports while regulating record availability, data transfer over the Internet, etc. In paper 3, they have offered direction for the application of blockchain technology to create a more reliable and secure IoT model. The functionality added by blockchain technology through the APIs provided by network nodes or by any specialized intermediaries would undoubtedly benefit the Internet of Things. They have given an overview of blockchain technology, discussed security concerns in the IoT context, and suggested blockchain as a solution for IoT security. In paper 4, they introduced a novel QHF-based cybersecurity technique created by quantum-inspired quantum walks. The proposed protocol used to construct a quantum-inspired blockchain for the safe transfer of data among IoT devices for smart water utilities took into account the necessity for privacy and secrecy in IoT devices for smart water utilities. The fundamental benefit of this research is that it provides a framework for developing blockchain solutions that can withstand potential attacks from both digital and quantum computers. Finally in paper 5, they employed a machine learning technique to analyze a sizable IoT dataset in order to identify IoT network assaults. The suggested methodology shows how the Hdoop-Spark cluster can be used to analyze big data and train an IoT intrusion detection machine learning model using a large dataset.
With the above discussion we can see many techniques and models which can be used to detect and mitigate many network attacks on IoT devices to safeguard our data and system.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

IV. CONCLUSION

In conclusion, these five research papers discuss numerous issues and issues related to the Internet of Things (IoT) implementation in diverse scenarios. Through the use of machine learning, blockchain technology, and cybersecurity methods inspired by quantum mechanics, they provide various solutions for improving the security, dependability, and efficiency of IoT devices. The papers emphasize the significance of creating new models and protocols to identify and stop potential network intrusions while protecting the privacy and confidentiality of data sent between IoT devices. Overall, the papers offer useful information about the current status of IoT research and development as well as suggestions for future research and applications.

REFERENCES

[1]- Internet of Things Security model available online at https://www.businessnewsdaily. com/4858-internet-of-things-will-change-work.html
[2]- Comparing Prototype Platforms: Arduino, Raspberry Pi, BeagleBone, and Launchpad available online: https: //www.electronicproducts.com/comparing-prototype-platforms-arduino-raspberry-pi-beaglebone-and-launchpad/
[3]- ShalaginovA., Kotsiuba, I.; Iqbal, A. “Cybercrime Investigations in the Era of Smart Applications: Way Forward Through Big Data”, Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, pp. 4309–4314, 2019
[4]- Cyberattacks on IOT Devices Surge, “Measured in Billions” available online: https:// www.oodaloop.com/briefs/2019/09/16/cyberattacks-on-iot-devices-surge-300-in-2019-measured-in-billions-report-claims/
[5]- Arshad, J.; Azad, M.A.; Abdellatif, M.M.; Rehman, M.H.U.; Salah, K. “COLIDE: A collaborative intrusion detection framework for Internet of Things. IET Netw”. 2019.
[6]- Karpatne A., “Theory-guided data science: A new paradigm for scientific discovery from data,” IEEE Transactionon Knowledgeand Data Engineering, vol. 29, no. 10, pp. 2318–2331, 2017.
[7]-Al-Turjman and S. Alturjman, “Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications,” IEEE Transition Industrial Information, vol. 14, no. 6, pp. 2736–2744,2018.
[8]- Dilberoglu M.D.,Gharehpapagh B.,Yaman U., and Dolen M., “The role of additive manufacturing in the era of industry 4.0,” Procedia Manuf., vol. 11, pp. 545–554, 2017.
[9]- Garg S.,Kaur K., Kumar N., and J. J. Rodrigues, “Hybrid deep-learningbased anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective,” IEEE Transition Multimedia, vol. 21, no. 3, pp. 566–578, 2019.
[10]- Ustundag A. and Cevikcan E., Industry 4.0: “Managing the Digital Transformation. Berlin, Germany: Springer”, 2017.
[11]- Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." Internet of Things (WF-IoT), 2014 IEEE World Forum.
[12]- Atzori, and Morabito, “The internet of things: A survey”, Computer Networks, 54(15), 2787–2805, 2010.
[13]- Humayed, Abdulmalik, "Cyber-Physical Systems Security—A Survey." arXiv preprint arXiv:1701.04525 (2017).
[14]- Meinel, Holger, and Wolfgang Bösch, "Radar Sensors in Cars." Automated Driving. Springer International Publishing, 2017. 245-261.
[15]- Uden, Lorna, and Wu He, "How the Internet of Things can help knowledge management: a case study from the automotive domain," Journal of Knowledge Management 21.1 (2017).
[16]- Sot iriadis, Stelios, Kostantinos St ravoskoufos, and Euripides GM Pet rakis, "Future Internet Systems Design and Implementation: Cloud and IoT Services Based on IoT-A and FIWARE." Designing, Developing, and Facilitating Smart Cities, Springer International Publishing, 2017.
[17]- Abd EL-Latif, A. A., Abd-El-Atty, B., Abou-Nassar, E. M., & Venegas-Andraca, S. E. (2020). “Controlled alternate quantum walks based privacy preserving healthcare images in internet of things”. OptLT, 124, Article 105942.
[18]- Abdullah, N., Hakansson, A., & Moradian, E. (2017). “Blockchain based approach to enhance big data authentication in distributed environment”. In 9th International Conference on Ubiquitous and Future Networks, ICUFN 2017 (pp. 887–892). Milan, Italy: IEEE Computer Society. 2017.
[19]- Al Ridhawi, I., Kotb, Y., Aloqaily, M., Jararweh, Y., & Baker, T (2019). “A profitable and energy-efficient cooperative fog solution for IoT services”. IEEE Transactions on Industrial Informatics, 16(5), 3578–3586.
[20]- Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). “A survey on blockchain for information systems management and security”. Information Processing & Management, 58(1), Article 102397.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

[21]- Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M., & Al Ridhawi, I. (2020). "An incentive-aware blockchain-based solution for internet of fake media things". Information Processing & Management, 57(6), Article 102370.
[22]- R. Genuer, J. M. Poggi, and C. Tuleau-Malot, "Variable selection using random forests", Pattern Recognition Letters, Vol. 31, Issue 14, 2010.
[23]- M.A. Ferrag and L. Maglaras, DeepCoin: "A novel deep learning and blockchain-based energy exchange framework for smart grids". IEEE Transactions on Engineering Management, 67(4), 1285-1297, 2020.
[24]- Reportlinker, "Internet of Things (IoT) Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)".
[25]- Sharma V., Lee K., Kwon S., Kim J., Park H., Yim K., Lee S.Y., "A Consensus Framework for Reliability and Mitigation of Zero-Day Attacks in IoT", Security and Communication Networks", vol. 2017, Article ID 4749085, pp.1-24, 2017.
[26]- Doshi R., Apthorpe N. and Feamster N., "Machine Learning DDoS Detection for Consumer Internet of Things Devices," 2018 IEEE Security and Privacy Workshops (SPW), pp. 29- 35,2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

SJIF: 8.423

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details