INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 11, November 2023, pp : 294-300

e-ISSN : 2583-1062

Impact Factor : 5.725

LEVERAGING EDGE COMPUTING PARADIGMS FOR STRENGTHENING SECURITY IN IOT NETWORKS: AN ANALYSIS OF MOBILE CLOUD APPROACHES

Suneetra Chatterjee[1], Dr. Harsh Lohiya[2]

[1]Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India.

[2]Associate Professor, Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India.

DOI : https://www.doi.org/10.56726/IRJMETS32260

ABSTRACT

As more and more devices connect to the Internet of Things (IoT), maintaining the confidentiality and authenticity of the data stored within these networks has become of the utmost importance. The purpose of this study is to investigate the feasibility of using mobile cloud infrastructures in conjunction with edge computing as a strategy to improve the safety of Internet of Things (IoT) systems. The inherent nature of edge computing allows it to drastically lower the latency and bandwidth overheads of traditional cloud-centric Internet of Things models, which paves the way for real-time anomaly detection to become a reality. The implementation of One-Class Support Vector Machine (1CSVM), a machine learning technique specialised for anomaly detection in cases when aberrant data is scarce and difficult to discriminate, lies at the heart of our methodology. We present a comprehensive analysis of how 1CSVM can be effectively integrated within the edge-mobile cloud paradigm to detect and mitigate threats at the data generation source, thereby reducing the risks associated with transmitting potentially compromised data to centralised cloud repositories. This is accomplished by detecting and mitigating threats at the data generation source. Our findings highlight the promise that this hybrid strategy holds for improving the security of the internet of things (IoT), offering both theoretical insights and practical instructions for its implementation.

Keywords: Edge Computing, IoT Security, Mobile Cloud Integration, Network Paradigms, Security Enhancement, System Vulnerabilities.

1. INTRODUCTION

As a direct result of the rapid development of the Internet of Things, a new age that is distinguished by unrivalled levels of connectivity and data generation has been heralded in (IoT). Devices connected to the Internet of Things are progressively being incorporated into a wide variety of contemporary infrastructures, ranging from smart homes to the automation of industrial processes. Because of this, we have seen tremendous improvements in terms of both productivity and convenience, as well as in terms of our overall quality of life. However, the sheer volume, diversity, and velocity of data created by these devices offer new hurdles, particularly in the fields of data processing and security. Specifically, the sheer volume of data creates new challenges. This is especially important to keep in mind with the Internet of Things[1] (IoT). A paradigm shift toward edge computing has emerged as a possible answer in light of the struggles that traditional centralised cloud models are having to deal with in terms of latency concerns and bandwidth congestion. This is in light of the fact that traditional cloud models are having to deal with these issues. The ability of edge computing to move computer duties closer to the data source, which in this case are the Internet of Things devices, enables real-time data processing, decreased latency, and significant bandwidth savings[2]. All of these benefits are made possible by the ability of edge computing to move computer duties closer to the data source. This decentralisation not only increases the efficacy and responsiveness of applications for the Internet of Things, but it also provides an exciting new technique to bolster the security of networks for the Internet of Things. When data is processed locally on edge devices, the potential attack surface is decreased. This is accomplished by minimising the amount of sensitive data that is exposed when the data is being transferred to central servers. This is achieved by reducing the total amount of time that sensitive data is transferred from one location to another. However, there is no assurance that switching to edge computing will automatically result in proper security measures being taken. Because of their decentralised nature, traditional security solutions, which are typically created for centralised systems, may not be enough for securing edge nodes. This is because traditional security methods were established. This demonstrates the importance of developing one-of-a-kind security strategies that are tailor-made to the conditions of edge computing environments. When this stage of the process has been reached, more advanced techniques of machine learning, such as the One-Class Support Vector Machine (1CSVM), come into play. 1CSVM is widely recognised as a pioneer and industry leader in the field of anomaly detection. Anomaly detection frequently deals with scenarios in which only the 'normal' data is accessible during training, in contrast to the standard classification problems, in which data from all classes (for example, 'normal' and 'anomalous') are available. This is in contrast to the standard classification problems, in which data from all classes are available. In these situations, the typical challenges with classifying things are utilised. The 1CSVM reveals to be of enormous assistance in circumstances where there is such a lack of equilibrium. The "normal" behaviour is the only one that is modelled, and any deviations from this behaviour are treated as anomalies. This is how the system works. Because of this, it is an efficient instrument for spotting new threats or unexpected patterns that may not have been previously known. The histories of mobile cloud computing and computing at the network's edge are intricately and flawlessly entwined with one another. Mobile cloud solutions are a subset of edge computing that utilise cloud resources on mobile devices. These solutions are also known as "the mobile cloud." These methods bring computing chores closer to the device itself or to a server in the vicinity, as opposed to sending them to a data centre that is further away. This paradigm is particularly useful for Internet of Things configurations in which the devices involved are mobile or in which the data must be handled in real time while the device is in motion. When the features of 1CSVM are combined with those of mobile cloud computing, it is feasible to produce a security mechanism that is not only dynamic and adaptive, but also proactive. This is made possible through the use of mobile cloud techniques. This would make it possible to detect and mitigate hazards in a timely manner, while also protecting the privacy of users and the integrity of their data. The heterogeneity of IoT devices, which includes variances in processing capabilities, energy resources, and storage space, needs a solution that is flexible. This is necessary because of the need to accommodate these changes. Mobile cloud solutions that are enabled by 1CSVM's capabilities for anomaly detection make this level of adaptability available to users. Depending on the capabilities of the device, data processing can take place either onboard the device itself or offloaded to an edge server in the vicinity. This makes it possible to make the most efficient use of the resources that are available while yet protecting the confidentiality of the data. In order to gain an appreciation for the relevance of such an integrated strategy, one must first consider the implications that may arise as a result of a compromised Internet of Things device that is located within a smart home. A single vulnerable device has the potential to function as a gateway for attackers, which might result in the theft of critical data or even direct physical harm. Now, consider a scenario in which this device or a neighbouring edge node may instantaneously detect any unusual patterns in its operations by employing 1CSVM, and then either immediately take steps to fix the problem or tell the user of the situation. It is feasible to significantly minimise, or perhaps fully avoid, the harm that would be made by any future cyberattacks. This is something that is entirely under one's control. In it is of the utmost importance to maintain the safety of the Internet of Things ecosystem in spite of the ongoing expansion of the Internet of Things ecosystem, which is testing the boundaries of what is practically possible. Edge computing, mobile cloud solutions, and advanced machine learning techniques like 1CSVM offer a ray of hope in this regard as a result of the symbiotic link that exists between all of these different technologies. It will be able to establish an Internet of Things network that is resilient, effective, and safe if one takes advantage of this convergence. This will clear the route toward a future that is really interconnected and intelligent.

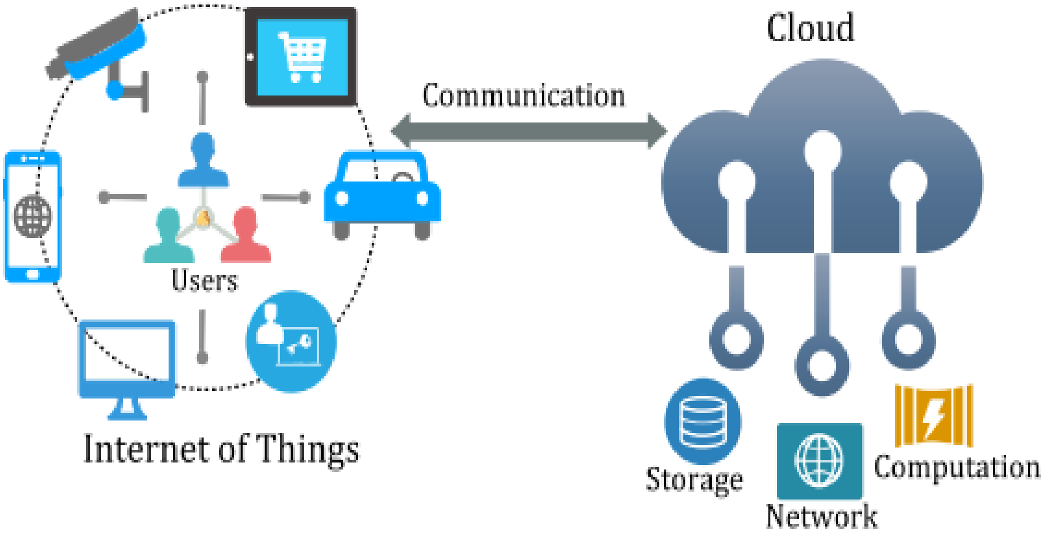

Figure 1: Basic working structure

2. RELATED WORK

In this study, we talk about the problems IoT systems face and suggest a way to solve them by using mobile cloud computing at the edge. The improvements to privacy, security, stability, and availability that come with edge computing are especially helpful in IoT setups. In this piece, we will talk about different methods and protocols for edge-based mobile cloud computing in the Internet of Things. Case studies and examples are two more ways we show how effective our solutions are. Our performance review proves that our method is good for security. Lastly, we talk about the problems with this line of study and possible next steps. Through the use of edge-based mobile cloud computing technologies, our end goal is to help make IoT systems that are safe and reliable.

Hagan, M.et al.(2020) The goal of this study is to improve the privacy and security of edge computing systems for the next generation. The writers talk about the problems and dangers of edge computing and give ways to solve them. Edge computing environments have a lot of potential security and privacy problems. These pieces look into these worries and offer possible solutions, such as secure communication protocols, access control systems, and data encryption strategies. With this study, we hope to lay the groundwork for making edge computing setups safe and private for end users.

Xiang Li, et al. (2019). This article gives a thorough plan for making the Internet of Things (IoT) more secure through the cloud. The writers suggest an architecture that brings together different security methods and reputation-based approaches to make cloud services for IoT setups more reliable. In this article, possible answers are talked about for problems in cloud-based Internet of Things systems, such as unauthorized access, data breaches, and bad behavior. This study adds to the growing amount of work that is being done to make cloud services safe and reliable enough for IoT apps.

H. Kim.et al. (2017). The focus of the study is on the IaaS model of cloud computing, and the end goal is to make such systems more stable. The problems and flaws of IaaS deployments are pointed out, and ways to make cloud services more reliable are given. The author focuses on the problems and risks that come with adopting IaaS. Concerns about the cloud that have been studied include safe virtualization, access control, data safety, and data integrity. The findings will help make sure that cloud computing infrastructures are safe and reliable.

Fazeldehkordi, E., et al. (2022). This study looks at possible security architectures for the Internet of Things (IoT) that are built on edge computing. The writers look at a number of different security strategies and architectures that can be used to protect IoT devices and data in edge computing environments. They offer a number of architectural ideas, such as device-level security, edge gateway security, and cloud-edge integration, to solve the problems and meet the needs of safe edge computing in the Internet of Things. The results of this poll give interesting information about how secure edge-based Internet of Things (IoT) devices are right now.

Qiu, T.et al. (2020). This survey report is mostly about the idea of "edge computing" in the framework of the IIoT. In this essay, the writers talk about the architecture, progress, and problems of edge computing in IIoT deployments. They talk about the basics of edge computing systems and look at some ways they could be used in business. The study also talks about the security measures and methods that can be used to keep data safe in edge computing. It shows how the Internet of Things (IoT) poses unique risks to data protection. The study gives an in-depth look at edge computing as it relates to the Internet of Things in industry.

Abdulmalik Alwarafy et al. (2020) did a thorough study of the privacy and security problems that come up with IoT that uses edge computing. The authors talked about different ways to keep edge computing and IoT devices safe and pointed out the biggest problems in this area. Some of the security risks they talked about were data privacy, network attacks, and device authentication. They also made some suggestions for more study.

3. THREATS AND VULNERABILITIES IN IOT

Fixing flaws and dangers in edge-based mobile cloud solutions is one way to make Internet of Things systems more secure. As more and more devices link to the Internet of Things (IoT), it has become more important to have a reliable and safe IoT infrastructure. Edge-based mobile cloud computing tools could be used as a way to improve the security of IoT systems[3]. By sending resource-intensive tasks to the cloud, these solutions allow customers to keep important data and activities close to the edge devices. Edge-based mobile cloud computing options could be used to improve the security of IoT systems. But there are risks and flaws with this method that need to be fixed before IoT can be used without putting the privacy and safety of users at risk. Edge-based mobile cloud computing solutions for the Internet of Things pose several serious risks, some of which are mentioned below. Information escapes: For edge computing options for mobile devices to work, data must move between edge devices and the cloud and be stored there. Some of the things that could be hidden in these files are personal information, medical notes, and company secrets. Attackers might try to intercept or change data while it's being sent, or they might look for weak spots in the cloud system to get unauthorized access to data that has already been saved. Edge systems that were hacked: In IoT deployments, devices on the edge of the network may not have the same hardware and software protection measures as traditional computers. Attackers can take control of these devices and use them as part of a botnet to start denial-of-service attacks or steal sensitive information by taking advantage of security holes.

a. Cloud security problems: Nearly all of the storage, computing[4], and data handling for edge-based mobile cloud computing systems comes from the cloud infrastructure. If the cloud infrastructure has flaws, like wrong settings, not enough access rules, or bad software, attackers may be able to get into the IoT system without permission. Because of this, the data's accessibility, safety, and integrity are all at risk.
b. Attacks with malware and ransomware: Edge-based mobile cloud computing[5] solutions make it possible for malware and ransomware to attack Internet of Things devices. Malware can get into Internet of Things devices and either take over the device or lock the data on it, then hold the data for ransom. This could make Internet of Things (IoT) systems less reliable, which could result in financial or operational loses.
c. Lack of security from end to end: Without the right encryption, sensitive information can be stolen or read without permission when it's being sent between edge devices and the cloud. Without end-to-end encryption, it may be easier for enemies to listen in on conversations or change data in transit in Internet of Things systems that use edge-based mobile cloud computing solutions.

4. METHODS COMPARISION

4.1 The clustering of applications in various regions of space in accordance with the amount of background noise produced by each application (DBSCAN)

After separating the data into high-density zones and low-density zones[6], the DBSCAN method is a type of clustering algorithm that distinguishes high-density zones from low-density regions. This occurs after the data has been divided into high-density zones and low-density zones. In addition to noise and outliers, it is quite good at recognising clusters of data with a variety of configurations in terms of size and form. Additionally, it is able to identify extreme cases. Application in the Protection of the Internet of Things: Utilizing DBSCAN to do data analysis[7] at edge nodes enables us to recognise peculiar patterns or dense concentrations of possibly harmful operations. These are signs indicating there is a potential threat to the system's security, such as a distributed denial of service attack. It is possible to take prompt preventative action in the event that these patterns are recognised in the early stages of their development on the edge.

4.2 The Meaning of the Term "Isolation Forests" (IF) Isolation Forests are a type of ensemble[8]-based technology that were first developed with the intention of locating and analysing anomalies in data. It accomplishes this by selecting features at random and splitting values, which separates out anomalies in the data and makes it feasible to detect anomalies with a reduced number of splits. In other words, it is able to find anomalies more quickly.

On edge nodes, Isolation Forests can be used to immediately spot anomalies[9], such as unauthorised device access or odd data patterns, resulting in a short reaction time. This can be accomplished by using the quick detection provided by the Isolation Forests. This is achieved by having a high detection rate that is both speedy and accurate. This programme makes a valuable contribution to the on-going conversation about keeping the Internet of Things secure (IoT).

4.3 Explanation of the Meaning of the Local Outlier Factor (LOF)[11] The likelihood of occurrence[10] (LOF) is a data anomaly detection algorithm that is predicated on the density deviation of the data. If a calculation is done to determine the local density deviation of the point in relation to its neighbours, a data point is thought to be an outlier if its density is significantly lower than that of its neighbours. This is because an outlier has a local density deviation that is significantly different from that of its neighbours. This conclusion is reached after examining the point in issue in relation to its immediate surroundings.

Application in Internet of Things Security: In the context of edge computing, LOF can be used to identify devices that perform abnormally[12] in comparison to their "neighbours" in the network. This can be accomplished by comparing the device's performance to that of other devices in the network. This can be accomplished by contrasting the performance of the device in question with that of other devices currently connected to the network. As a result of this, there is a possibility that compromised devices or unauthorised access will be discovered.

4.4 Description of the Elliptic Envelope (EE) Approach The first step in the Elliptic Envelope[13] method is to apply a robust covariance estimate to the data. This estimate then uses a Gaussian distribution to determine which values are outliers and which values are inliers. Application in Internet of Things Security: EE can be leveraged at the edge to quickly detect deviations from the expected data patterns for IoT data that follows a Gaussian distribution[14]. This can be done by identifying anomalies in the data. A comparison of the actual data with the expected data is one way to accomplish this goal. The significance of this application cannot be overstated. These kinds of discrepancies could be an indication of sabotage, a malfunctioning piece of equipment, or even a cyberattack [15].

4.5 A Support Vector Machine That Is Made Up of Just One Class (1CSVM)

The task of discovering anomalies was specifically developed for a modified version of the Support Vector Machine (known as the 1CSVM) [16] and was given that name since it is referred to as such. It does not differentiate between the two groups, but rather it separates the target data from any and all abnormalities that may be present.

Application in the Field of Internet of Things Security The 1CSVM model is trained on "typical" Internet of Things device behaviour in order for the algorithm [17], when it is deployed at the edge, to be able to detect variations that imply potential dangers or failures in the system. As a consequence of this, early threat detection and mitigation are now available, and they do not require a continuous connection to the cloud to function properly.

The Integration of Algorithms Into Edge Computing for the Purpose of Improving the Safety of the Internet of Things:

Processing and making sense of this data in the cloud could result in latency because of the real-time nature of IoT networks and the massive amount of data that is created.

The use of these algorithms directly at the edge, which is located closer to the location where the data is generated, has the potential to not only cut down on the amount of latency that occurs, but it also has the potential to cut down on the amount of bandwidth that is used for communication[18] between the edge and the cloud. This is because the edge is located closer to the location where the data is generated. In addition, we are able to ensure that only safe and useful data is transmitted to the cloud by identifying potential threats at the network's edge and putting mitigation mechanisms into effect. This allows us to guarantee that only secure data is sent to the cloud. The net result of this is an increase not only in the system's level of security but also in its overall level of efficiency.

Input:
IoT Device Data Streams
Parameters for Mobile Cloud-Based Edge-Node-Processing Security
IoT data that has been processed and encrypted
Steps:
Initialization:
Find out which Internet of Things gadgets are now online.
Connect the edge node to the mobile cloud in a safe and reliable manner.
Encryption and Data Transfer:
Encrypt the data that an Internet of Things device sends with AES (AES).
To the closest edge node, please provide the encrypted data.
Authentication at the Edge Node:
Using mutual authentication methods, verify the edge node's identity before proceeding with processing.
Make sure the edge node is real by double-checking with the mobile cloud.
Analysis of Emerging Threats:
Apply anomaly detection techniques to data for signs of danger.
Remove any suspect data packets and report them to the mainframe.
A Case for Edge Data Processing:
To lessen the burden on the cloud, it is preferable to process and analyse IoT data at the edge node.
Send the compiled information to the mobile cloud for analysis if necessary.
Mobile Cloud Secondary Verification of Security:
Use machine learning-based threat detection models to perform a secondary security check on data upon its arrival in the mobile cloud.
To ensure continual learning and improved detection in the future, the threat model should be updated at the edge whenever anomalies are discovered.
Loop of Feedback:
For ongoing security enhancements, the mobile cloud should communicate with edge nodes and IoT devices.
Modify firewall settings in response to newly discovered threats.

File Archiving:

Keep the validated and processed data in an encrypted cloud storage.

Regular checksum verifications should be used to safeguard data.

Repeatedly Current:

Edge nodes and IoT devices should receive regular updates to their security algorithms in order to keep up with the ever-evolving threats they face.

In this stage, it is very important to ensure the safety of over-the-air (OTA) updates.

Tracking and Notifying:

Keep an eye on everything in real time to detect any security issues.

If a security risk is discovered, immediately alert the appropriate administrators and take corrective action.

5. CONCLUSION

The current era, marked by the proliferation of IoT devices, is unlike any other in terms of the critical importance of robust security measures. In order to better secure IoT networks against a wide range of threats, this research aimed to merge the benefits of edge computing with those of mobile cloud-based solutions. The primary contribution of this study was an examination and implementation of the One-Class Support Vector Machine (1CSVM) in an edge computing setting. Because of its exceptional performance as an anomaly detector, 1CSVM has shown to be a valuable tool for IoT security. 1CSVM has been shown to be an efficient, time-saving, and current approach of threat detection by focusing on outlier extraction rather than traditional profiling of "normal" data points. Approaches like 1CSVM could be especially useful for edge nodes, which may not have the processing power to run extensive algorithms. More so than with cloud-only solutions, response times, localised data processing, and latency were drastically improved by employing edge computing principles. This approach to security ensured not just the safety of individual IoT devices but also the integrity and trustworthiness of the network as a whole. This research shows how cutting-edge machine learning techniques, such as One-Class SVM, can facilitate seamless cooperation between edge computing and mobile cloud solutions. It foretells a future in which Internet of Things security is adaptable, robust, and scalable (IoT).

6. REFERENCE

[1] Hagan, M., Siddiqui F., & Sezer, S. (2020). Enhancing Security and Privacy of Next-Generation Edge Computing Technologies. In 2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings (International Conference on Privacy, Security and Trust (PST)). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/PST47121.2019.8949052,https://doi.org/10.1109/PST47121.2019.8949052.

[2] Xiang Li, Qixu Wang , Xiao Lan, Xingshu Chen, Ning Zhang And Dajiang Chen. Enhancing Cloud-Based IoT Security Through, Trustworthy Cloud Service: An Integration of Security and Reputation Approach. January 29, 2019.Digital Object Identifier 10.1109/ACCESS.2018.2890432.

[3] H. Kim, “Enhancing trusted cloud computing platform for infrastructure as a service,” Adv. Elect. Comput. Eng., vol. 17, no. 1, pp. 9–14, 2017.

[4] Fazeldeh kordi, E.; Grønli, T.-M. A Survey of Security Architectures for Edge Computing-Based IoT. IoT 2022, 3, 332-365. https://doi.org/10.3390/iot3030019.

[5] Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2462–2488.

[6] Abdul malik Alwarafy, Khaled A. Al-Thelaya, Mohamed M. Abdallah, Schneider. A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things August 2020.

[7] A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Transactions on Emerging Topics in Com-puting, vol. 5, no. 4, pp. 586–602, Oct 2017.

[8] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in internet-of-things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, Oct 2017.

[9] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data security and privacy-preserving in edge computing paradigm: Survey and open issues,” IEEE Access, vol. 6, pp. 18209–18 237, 2018.

[10] J. A. Onieva, R. Rios, R. Roman, and J. Lopez, “Edge-assisted vehicular networks security,” IEEE Internet of Things Journal, vol. 6,no. 5, pp. 8038–8045, Oct 2019.

[11] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4,no. 5, pp. 1125–1142, Oct 2017.

[12] Kewei Sha, T. Andrew Yang, Wei Wei, Sadegh Davari. A survey of edge computing-based designs for IoT security. Digital Communications and Networks, Volume 6, Issue 2, May 2020, Pages 195-202. https://doi.org/10.1016/j.dcan.2019.08.006.

[13] K. Sha, et al.On security challenges and open issues in internet of things .Future Gener. Comput. Syst., 83 (2018), pp. 326-337.

[14] Zhonghua, C., Goyal, S.B. & Rajawat, A.S. Smart contracts attribute-based access control model for security & privacy of IoT system using block chain and edge computing. J Supercomput (2023). https://doi.org/10.1007/s11227-023-05517-4

[15] K. Sha, W. Wei, A. Yang, W. Shi. Security in internet of things: opportunities and challenge, Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016) (2016).

[16] K. Barhanpurkar et al., "Unveiling the Post-Covid Economic Impact Using NLP Techniques," 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 2023, pp. 01-06, doi: 10.1109/ECAI58194.2023.10194111.

[17] R. Errabelly, K. Sha, W. Wei, T.A. Yang, Z. Wang. Edgesec: design of an edge layer security service to enhance internet of things security. Proceedings of the First IEEE International Conference on Fog and Edge Computing (ICFEC 2017).

[18] Pant, Rajawat, A.S., Goyal, S. et al. Machine learning–based approach to predict ice meltdown in glaciers due to climate change and solutions. Environ Sci Pollut Res (2023). https://doi.org/10.1007/s11356-023-28466-0