IoT Systems Security Enhancement: Evaluating the Interplay between Mobile Cloud Solutions and Edge Computing Techniques

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

ABSTRACT

As the number of IoT-enabled gadgets continues to mushroom, so does the urgency of the issue of ensuring their safety. Edge-based mobile cloud computing is a paradigm that can be used to increase the security of IoT systems (EMCC). In this abstract, we will discuss the function of EMCC technologies in improving the safety of the IoT. (IoT). EMCC leverages the processing speed and storage space provided by edge devices and cloud resources to address the challenges posed by security threats in IoT settings. By moving processing closer to the network's edge, EMCC reduces the volume of data sent to the cloud. This not only improves privacy but also helps minimise latency. Using a decentralised approach lessens the chance that private data will fall into the wrong hands. To further strengthen the safety of IoT devices, EMCC employs state-of-the-art security methods. Edge infrastructure is equipped with safeguards such secure data aggregation, cryptographic algorithms, and access control mechanisms to preserve data availability, integrity, and confidentiality. Effective key management and authentication methods are essential for securing communications between IoT devices, edge nodes, and cloud servers, and EMCC facilitates their deployment. In addition to the security benefits, EMCC also boosts the overall performance of IoT devices. By moving computation to the network's periphery, it reduces the burden on limited-capacity IoT devices, allowing them to consume less power and last longer. In addition, this alleviates user anxiety. Increases in Internet of Things deployments can be made without disrupting service or compromising data security thanks to the scalability of cloud resources. The emphasis of this abstract is on the potential value of EMCC to enhance the security of IoT systems. Future Internet of Things deployments may want to consider EMCC as a viable alternative because it not only improves performance by combining edge computing and cloud resources, but also tackles security concerns. Because of this, EMCC is a great option to consider.

Keywords: *IoT Systems , Security Enhancement , Mobile Cloud Solutions , Edge Computing , Interplay .*

1. INTRODUCTION

The Internet of Things, which is also referred to as IoT on occasion, has brought about a dramatic shift in the field of digital innovation. These interconnected devices, which can be as basic as thermostats found in homes or as complicated as sensors used in commercial and industrial settings, are reshaping the way in which we interact with the wider world around us. They offer a level of automation, simplicity, and efficiency in their goods that is unmatched by their competitors. On the other hand, the proliferation of connected devices connected to the Internet of Things (IoT) simply serves to make the security issues that already exist worse. The greater the variety of connections that are being supported, the higher the probability that there may be flaws in the system or malicious attacks. One of the most fundamental challenges in safeguarding the Internet of Things is posed by the sheer number and variety of the many devices (IoT). A good many of these devices have limited computational capabilities, and their utility, rather than their safety, is typically prioritised during the development process, such that usefulness is often prioritised over safety. The goal of delivering uniform security requirements within an ecosystem that is both broad and diverse is a difficult one to accomplish. This problem is made even more difficult by the fact that these devices constantly send and receive data, which makes them vulnerable to attacks such as data breaches and illegal access. Additionally, this problem is made more difficult by the fact that these devices are constantly connected to

the internet. Traditionally speaking, the majority of the data processing and analytics related with IoT devices have been offloaded to centralised cloud services. This is expected to change in the near future. There are some great characteristics of this paradigm; however, there are also some unfavourable aspects that should be taken into consideration. The transmission of data to a centralised cloud for the purpose of processing causes latency and presents a potential bottleneck in circumstances that need instantaneous answers. The transmission of data across extensive distances significantly increases the risk that there will be security loopholes or violations. This is the most important aspect to consider. At this crossroads, solutions that are based on mobile cloud computing and computing at the network's edge come into their own as viable options. The purpose of edge computing is to process data in a location that is geographically closer to the source of the data, which in the context of the Internet of Things would be the devices themselves. Edge computing not only reduces latency by providing data processing at or near the IoT devices, but it also eliminates the risk that is associated with transmitting sensitive data across the network. This can be accomplished by providing data processing at or near the IoT devices. This is achieved by enabling data processing on or in close proximity to the Internet of Things devices. In a similar vein, mobile cloud solutions are an improvement over this paradigm since they take advantage of the computational power afforded by mobile devices. Taking advantage of these technologies enables Internet of Things devices to either process data locally or offload it to a mobile device or edge server that is positioned in close vicinity. This method maximises the use of available resources, shortens reaction times, and further improves the security framework by imposing limitations on the transit of data. It also reduces the amount of time it takes to complete tasks. Despite the undeniable truth that these architectural adjustments improve security, a more proactive and sophisticated defence mechanism is still required because of the ever-changing nature of cyber threats. This is because cyber attacks can take many different forms. You are going to move on to the next frontier, which is machine learning, and more specifically the One-Class Support Vector Machine (1CSVM). In contrast to traditional binary classifiers, which require information from both the "normal" and "anomalous" classes, the 1CSVM was designed expressly for situations in which only the "normal" class is prevalent. This is because traditional binary classifiers require information from both classes. As a result of this, 1CSVM is an extremely powerful tool for anomaly detection, particularly in the context of the internet of things (IoT), where recognised threat patterns may be few, but undiscovered dangers may be numerous. In this context, 1CSVM is particularly useful because it can detect anomalies in large amounts of data very quickly. 1CSVM models the "usual" behaviour of IoT devices, and any deviations from this norm that are deemed to be potential irregularities or risks are recognised and identified by the system. This method is more adaptable and successful than relying only on known danger signatures, which is something that should be kept in mind given the dynamic nature of the threats provided by the internet of things (IoT). It is possible for 1CSVM to provide real-time threat detection and response when it is incorporated into the edge computing and mobile cloud framework. This, in turn, greatly minimises the window of risk that is present. Imagine if the infrastructure of a smart city includes an Internet of Things network, and that everything from the traffic lights to the waste management systems to the water supply is integrated. In a setting as essential as this one, any delay that occurs between the identification of a potential threat to security and the deployment of a response to that potential threat could result in significant disruptions or even devastating consequences. However, if each device or a cluster of devices is outfitted with the capability to detect anomalies in real-time through techniques such as 1CSVM, and if these devices also benefit from the localised data processing that edge computing provides, then the system as a whole will be more resilient to disruptions. As we get closer to the end of this introduction, it is vital to remember that as we move closer to a world controlled by IoT, the conventional security paradigms will need to be regularly reviewed. This is because we are getting closer to a world that will be dominated by IoT. This is because the Internet of Things is rapidly becoming more widespread. The confluence of edge computing, mobile cloud solutions, and strong machine learning methodologies such as 1CSVM represents a huge step forward in this journey. This synergy represents a significant step forward in this journey. It embodies the ability to not only defend against risks but also to forecast and preempt them, which will ensure that the promise of the internet of things is realised in its fullest and safest form. This will ensure that the promise of the internet of things is realised in its fullest and safest form.

2. RELATED WORK

Mosenia et al.(2017) did a lot of research on the topic of how to keep IoT gadgets safe. They looked into many IoT network weaknesses and entry places that could be used by hackers. The effects of these flaws on people's privacy were talked about, and several changes that could work were suggested. Their results showed how important it is to protect the Internet of Things (IoT) with things like encrypted data transfer, limited access, and detecting unusual behavior.

Yang et al. (2017) presented a survey that asked about worries about safety and privacy linked to the Internet of Things. They looked at the risks and weaknesses of IoT deployments and looked into a number of security choices, such as access control, authentication, and encryption. The writers emphasized how important it is to standardize security processes and tools to reduce risks.

Zhang et al. (2018) ran a poll to find out what people think about data security and privacy in edge computing. To make it possible to handle and store data securely at the edge, they looked at the problems and questions that still need to be answered. The authors gave and talked about a number of ways to keep personal information safe in edge computing, such as encryption, access control, and data anonymization.

Onieva et al. (2019) The problems with network security in edge-assisted vehicle networks were looked into. They looked at how Internet of Things applications in cars could have flaws that could be used in an attack. They also made sure that the privacy, availability, and security of in-vehicle interactions were protected. The authors of the paper stressed how important it is for vehicle networks to have trustworthy management and encrypted communication lines.

Lin et al. (2017) gave a thorough explanation of the IoT, from its basic parts to its possible weaknesses and uses. As part of their study, the authors looked at both the risks to privacy and the benefits of IoT setups. The pros and cons of putting IoT into place were also looked at. They also looked at possible answers and study directions for the future to make the IoT safer.

Sha et al. (2020) IoT security methods based on edge computing were looked into as part of a study. They talked about the pros and cons of using edge computing to improve the security of IoT. Some of the methods and approaches that the writers have looked at in depth are secure data aggregation, edge-based intrusion detection, and secure communication protocols. They also talked about how edge computing systems need to have security measures that work together.

K. Sha et al. (2018) looked into the many questions and worries about the security of the Internet of Things for which there are still no answers. In their study, they focused on the risks that come with IoT devices. Concerns about data protection, problems with authentication and access control, and attacks from bad people are all examples of these risks. The authors stressed that IoT rollouts need strict security measures to keep them safe.

Sha, et al. (2016) talked about the pros and cons of the IoT and how it could be used. They gave a review of the security needs of IoT systems and emphasized how important it is to make sure the data is available, correct, and private. This piece also talked about what's new in technology and what could be done to make the Internet of Things (IoT) safer.

Errabelly, et al .(2017) Edgesec was offered as a plan for an IoT security service at the edge layer. The goal was to make IoT security stronger. Their study was mainly about how to use the capabilities of edge computing to make good security processes for IoT devices that are closer to the edge. Edge computing has a lot of benefits for IoT deployments, including less latency, more scalability, and better security.

Hsu, et al. (2018) provided an Internet of Things security architecture that could be changed and was built on the edge. Their study showed that IoT settings need security methods that can change and adapt to the risks that are

always changing. The authors came up with a way to keep IoT devices and data safe by using computation at the edge of the network and the flexibility of reconfigurable security rules.

3. PROPOSED METHODOLOGY

The phrase "Density-Based Spatial Clustering of Applications with Noise" is what "DBSCAN" stands for in its full form.

DBSCAN is responsible for the organisation of the data into dense clusters, which are subsequently separated by zones that contain less data points. This is accomplished by identifying which data points are not related with any one of the clusters.

1. The DBSCAN application can be utilised to recognise unusual patterns in the flow of data when applied to the context of networks that are connected to the Internet of Things. If data points, which indicate behaviours of Internet of Things devices based on metrics such as'vent,' 'pluie,' and 'temp,' do not belong to any of the regular clusters, this may be a sign that there are potential security risks.

2. Isolation Forests (IF): The following is a description of a type of technique for detecting anomalies that is known as an isolation forest. The data space is divided recursively in order to find and isolate any anomalies, which is how it works.

Isolation as an Example of Application in Context When applied in a scenario involving edge computing, Forests are capable of efficiently separating anomalous data points generated by Internet of Things devices. Due to the fact that it can function efficiently with very large datasets, it is suited for use in networks that comprise a considerable number of Internet of Things devices.

3. The LOF, also known as the local outlier factor: The LOF is a metric that analyses the local deviation of a data point's density in comparison to the density of the points that are immediately surrounding the data point in question. It is able to recognise irregularities even when their densities are comparable to those of normal data points.

Application in Context: LOF can be utilised to help in finding local anomalies in data streams that are created by devices that are connected to the internet of things. It is especially helpful for discovering small security risks that may be missed by global outlier detection methods. This can be done by using a combination of both global and local data. Using this technology, one is able to attain the aforementioned goal.

4. Elliptic Envelope (EE): This method analyses the dataset by fitting a multivariate Gaussian distribution to it. It then determines which points are outliers by determining whether or not they fall outside the envelope of the distribution.

Application in Context: EE might be useful for datasets that have a Gaussian distribution, such as some environmental sensors in IoT that measure'vent,' 'pluie,' and 'temp,' as the following example demonstrates. It is able to detect sudden spikes or reductions in the signal, either of which may indicate that the signal has been tampered with or that there is a malfunction.

5. One-Class Support Vector Machine (commonly abbreviated as 1CSVM): 1CSVM is an unsupervised algorithm that has the ability to recognise abnormalities in data points that are located a great distance from the origin. In order to accomplish this goal, it first separates the data points in the feature space from the origin and then identifies the data points that are furthest away from the origin.

Application in Context The 1CSVM can be used in situations where the normal behaviour of the IoT network has been clearly outlined, and anomalies are defined as data points that depart significantly from this norm. Anomalies can be determined by comparing the data point to the norm, and then comparing the anomaly to the norm.

Visualization:

For each algorithm, visualizing the dataset in three dimensions ('vent', 'pluie', 'temp') will provide a clear distinction between normal data points and outliers. This visualization can aid in real-time monitoring, enabling swift security responses.

Using these algorithms in the context of the paper can offer a robust approach to identifying and mitigating potential security threats in IoT networks, further strengthened by edge computing paradigms.

1. Initialize the IoT device and edge cloud server.
2. Establish a secure connection between the IoT device and the edge cloud server.
3. Implement an encryption mechanism to protect the data transmitted between the IoT device and the edge cloud server.
4. Set up a firewall on the edge cloud server to filter and block unauthorized access attempts.
5. Develop a mechanism to detect anomalies in the IoT device's behavior, such as unexpected data transmission patterns or unauthorized access attempts.
6. Implement intrusion detection and prevention techniques on the edge cloud server to detect and respond to potential security threats.
7. Employ authentication and authorization protocols to ensure that only authorized users and devices can access the IoT system.
8. Implement access control mechanisms to restrict access to sensitive data and resources within the IoT system.
9. Set up a secure communication channel between the edge cloud server and the mobile cloud.
10. Apply secure data storage techniques to protect the stored data within the mobile cloud.
11. Employ secure data transmission protocols between the edge cloud server and the mobile cloud to ensure the confidentiality and integrity of data in transit.
12. Implement secure protocols for communication between the IoT device, edge cloud server, and mobile cloud.
13. Develop a mechanism to monitor and audit security events within the IoT system for detecting and responding to security incidents.
14. Regularly update and patch the software and firmware of the IoT device, edge cloud server, and mobile cloud to address any identified security vulnerabilities.
15. Continuously monitor and assess the security of the IoT system, identify potential weaknesses, and take proactive measures to enhance security.
16. Conduct periodic security audits and penetration testing to evaluate the effectiveness of the implemented security measures and identify areas for improvement.

The operation of the proposed strategy

The Explanation of Isolation Forests

A novel technique to anomaly detection, unsupervised learning can be accomplished with the help of isolation forests. Isolation Forests are an alternative to the traditional way of determining what constitutes "normal" behaviour and locating deviations from this norm. Instead, the emphasis of this method is placed on immediately isolating anomalous locations.

The following are some of the phases that can be used to summarise the methodology:

Random Feature Selection: For any given data point, a feature and a random value within the span of the selected feature are both chosen at random. This is known as the random feature selection method.

Comparison of Feature Values The value of the data point for the feature that was chosen is compared with a value that was chosen at random. If the value of the data point is higher, then the feature will have a new lower bound determined by the value that was picked. On the other hand, if it is lower, it creates a new upper bound for the range.

Isolation Verification: Determine if there is any other data point that resides within the altered feature bounds (from step 2) and also within the unmodified ranges of other features. This is part of the process of determining whether or not there is any other data point. If there is no other data point that fits the description, the first point will be considered isolated.

Iterative Isolation: Repeat the method from step 1 through step 3 as many times as necessary until the data point in question can be isolated. The "isolation number" of a point is equal to the number of iterations that must be completed before it can be considered isolated.

One of the most important takeaways from taking this technique is the realisation that aberrant observations are typically separated more quickly than conventional ones. Therefore, a smaller isolation number implies that there is a higher possibility that the observation is an outlier.

Data Streams from Internet of Things Devices: Gather information in real time from a wide variety of sensors, cameras, and other networked gadgets. System logs, transaction times, sensor readings, and operational statuses are all examples of possible data properties.

Retrieve past datasets from edge and cloud storage to use in One-Class SVM model training.

Preparing the Data:

Data cleansing entails eradicating anomalies and outliers that aren't actually hazards to security.

Extracting features that are representative of a device's behaviour is the focus of feature engineering. Improve SVM efficiency by standardising or normalising data.

Partitioning the Data: Separate the Data into Test and Training Sets. The test set can include both "normal" and "anomalous" data, with the latter perhaps being synthetically generated or based on existing instances; the training set should mostly comprise "normal" behavioural data.

Framework Establishment for Mobile Cloud and Edge Computing:

Deploy Edge Nodes: Place edge nodes in close proximity to IoT devices and supply them with adequate processing power.

Integrate mobile cloud platforms to perform computations locally or offload them to edge nodes in the area.

To Train a Model with Only One Class:

Select a suitable kernel for the SVM, such as the Radial Basis Function (RBF), according on the data's characteristics.

Hyperparameter Tuning entails employing optimization strategies like grid search and random search to fine-tune settings like the regularisation factor and the kernel coefficients.

The One-Class SVM may be trained to identify "normal" actions by utilising a training dataset.

Real-time Anomaly Detection

In order to deploy the learned One-Class SVM model, it must be used in conjunction with edge nodes and mobile cloud solutions.

Anomalies are detected using real-time monitoring, wherein data from IoT devices is continuously fed into a model.

Mechanisms for issuing warnings in the case of abnormalities being uncovered; these can be used to head off potential security breaches.

Analyzing the Model:

Evaluation of Model Performance: False Positive and True Negative Rates, as well as Area Under the ROC Curve (AUC-ROC).

Retrain and fine-tune the model based on the results of the feedback loop, which includes both false positives and negatives.

Integration and scaling in real time:

Scalability: Make sure the security architecture can manage more data and more processing as the number of IoT devices grows.

In order to keep up with shifting device behaviours and new security concerns, it is important to continuously integrate new data into the One-Class SVM model.

Reporting

Security Records: Keep complete records of all suspicious activity, including timestamps and connected Internet of Things devices.

Generate in-depth security reports on a regular basis detailing any vulnerabilities, threats, and countermeasures taken.

Results analysis

Dataset Name	Description	Features/Attributes
IoT Device Logs	Logs generated by IoT devices	Timestamp, Device ID, Event Type, Data
Network Traffic	Network traffic data captured	Source IP, Destination IP, Protocol, Port, Data Size
Anomaly Detection	Labeled dataset for anomaly detection	Sensor readings, Timestamp, Label
Intrusion Attempts	Records of detected intrusion attempts	Timestamp, Source IP, Destination IP, Attack Type, Result
User Authentication	User authentication logs	Timestamp, User ID, Login/Logout, Success/Failure
System Logs	Logs of system activities and events	Timestamp, Event Type, Event Details
Mobile Cloud Usage	Usage data of the mobile cloud	Timestamp, User ID, Data Usage, Resource Utilization
Vulnerability Database	Information about known vulnerabilities	Vulnerability ID, Description, Severity

Algorithmic Performance Comparison Using Custom Metrics

In this section, we delve into a comparative analysis of the algorithms based on a unique metric we've devised.

Our evaluation metric utilizes a reference data frame, named df_anomaly_reference, derived from our primary dataset. This reference frame specifically captures instances identified as outliers.

For each algorithm, predictions are juxtaposed against df_anomaly_reference to categorize them into:

True Negative (TN): Instances correctly identified by the algorithm as outliers.

False Positive (FP): Instances incorrectly marked as outliers by the algorithm, even though they aren't in reality.

For clarity, the annotations are as follows:

0 signifies non-outliers or positive instances.

1 indicates outliers or negative instances.

'True' implies the algorithm's prediction aligns with the actual status.

'False' denotes a mismatch in the algorithm's prediction and the real status.

Our analysis focuses on four select months: January, February, June, and July. The methodology remains consistent across these months; one merely needs to adjust the df_curr variable to evaluate a different month.

4. CONCLUSION

The Internet of Things (IoT) is a complicated environment that exemplifies the limitless possibilities and significant problems of a globally networked world. The importance of a balanced combination of mobile cloud solutions, edge computing approaches, and advanced machine learning, in particular One-Class Support Vector Machine (1CSVM), has become clearer as we have dove deeper into the complexities of IoT Systems Security Enhancement. Defending these pervasive networks against attacks is becoming increasingly important as the number of connected devices in the world continues to grow. The real-time and massive data processing needs of the Internet of Things have revealed weaknesses in the traditional centralised cloud platforms, which are robust in their own right. Edge computing has emerged as a crucial countermeasure since it allows for decentralised processing close to data sources. It not only speeds up data processing, but also protects sensitive information from being compromised in transit. Decentralizing processing does not, however, ensure bulletproof safety. Due to their location, edge nodes may be more vulnerable than other nodes. This is where the One-Class SVM really shines. 1CSVM provides a nuanced and preventative method of anomaly detection by first modelling "normal" behaviour and then looking for hazards hidden inside anomalies. In the ever-changing Internet of Things (IoT), where dangers are always evolving, such a system is essential. When combined with mobile cloud technologies, this integration significantly increases safety. At the intersection of edge and cloud computing, mobile cloud computing is able to dynamically adjust processing techniques in response to available device resources. By incorporating 1CSVM into this framework, every node, whether it's doing its own processing or being offloaded, may act as a sentry, keeping an eye out for any signs of a security breach. This study highlights a key discovery: the future of IoT security isn't just about more powerful firewalls or improved encryption, but also about the synergies between mobile cloud, edge computing, and 1CSVM. It's about encouraging flexibility, learning to recognise the standard in order to spot the unusual, and capitalising on the advantages offered by new forms of computation. Each component—device, network, and data packet—is essential to the whole of the Internet of Things. With the power of edge computing, mobile cloud solutions, and One-Class SVM, we can create an IoT ecosystem where innovation can flourish, protected from outside interference, and where connectivity is a source of strength rather than weakness.

5. REFERENCES

1. A. Mosenia and N. K. Jha, “A comprehensive study of security ofinternet-of-things,” IEEE Transactions on Emerging Topics in Com-puting, vol. 5, no. 4, pp. 586–602, Oct 2017.
2. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security andprivacy issues in internet-of-things,” IEEE Internet of Things Journal,vol. 4, no. 5, pp. 1250–1258, Oct 2017.
3. J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data securityand privacy-preserving in edge computing paradigm: Survey and openissues,” IEEE Access, vol. 6, pp. 18209–18 237, 2018.

4. J. A. Onieva, R. Rios, R. Roman, and J. Lopez, “Edge-assistedvehicular networks security,” IEEE Internet of Things Journal, vol. 6,no. 5, pp. 8038–8045, Oct 2019.
5. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A surveyon internet of things: Architecture, enabling technologies, security andprivacy, and applications,” IEEE Internet of Things Journal, vol. 4,no. 5, pp. 1125–1142, Oct 2017.
6. 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.
7. K. Sha, et al.On security challenges and open issues in internet of things.Future Gener. Comput. Syst., 83 (2018), pp. 326-337.
8. 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).
9. 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) (2017).
10. R. Hsu, J. Lee, T. Quek, J. Chen.Reconfigurable security: edge-computing-based framework for iot.IEEE Network, 32 (5) (2018), pp. 92-99.
11. Hushmat Amin Kar, G.M. Rather, "A Survey on Edge-Based Internet-of-Things", International Journal of Computer Networks and Applications (IJCNA), 6(6), PP: 100 - 109, 2019, DOI: 10.22247/ijcna/2019/190369.
12. Hamdan S, Ayyash M, Almajali S. Edge-Computing Architectures for Internet of Things Applications: A Survey. Sensors (Basel). 2020 Nov 11;20(22):6441. doi: 10.3390/s20226441. PMID: 33187267; PMCID: PMC7696529.
13. Jeon, G., Albertini, M., Bellandi, V. et al. Intelligent mobile edge computing for IoT big data. Complex Intell. Syst. 8, 3595–3601 (2022). https://doi.org/10.1007/s40747-022-00821-7.
14. Dr Suresha K, Suresh Goure, Shaheen Banu. A Comprehensive Review on Edge Computing. DOI Link: https://doi.org/10.22214/ijraset.2023.48484.
15. Al Masarweh M, Alwada’n T and Afandi W. (2022). Fog Computing, Cloud Computing and IoT Environment: Advanced Broker Management System. Journal of Sensor and Actuator Networks. 10.3390/jsan11040084. 11:4. (84). https://www.mdpi.com/2224-2708/11/4/84.
16. Brecko A, Kajati E, Koziorek J and Zolotova I. (2022). Federated Learning for Edge Computing: A Survey. Applied Sciences. 10.3390/app12189124. 12:18. (9124).https://www.mdpi.com/2076-3417/12/18/9124.
17. C.T. Meenatchi Sundaram and Dr. A.R. Mohammed Shanavas. Improving the QoS of Mobile Cloud Computing Applications in Smart Environments. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 11 (2017) pp. 2754-2760 © Research India Publications. http://www.ripublication.com.
18. X. Huang, R. Yu, J. Kang, and Y. Zhang, “Distributed reputationmanagement for secure and efficient vehicular edge computing and networks,” IEEE Access, vol. 5, pp. 25 408–25 420, 2017.

19. J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," IEEE Access, vol. 6, pp. 23 626–23 638, 2018.
20. J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," IEEE Network, vol. 33, no. 2, pp. 50–57, March 2019.
21.] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb,"Survey on multi-access edge computing for internet of things realization," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp.2961–2991, Fourthquarter 2018.
22. J. Ni, K. Zhang, X. Lin, and X. S. Shen, ''Securing fog computing for Internet of Things applications: Challenges and solutions,'' IEEE Commun.Surveys Tuts., vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.
23. Ugochukwu, N.A.; Goyal, S.B.; Rajawat, A.S.; Islam, S.M.N.; He, J.; Aslam, M. An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method. Mathematics 2022, 10, 4670. https://doi.org/10.3390/math10244670
24. A. Mohsenzadeh, H. Motameni, and M. J. Er, ''A new trust evaluation algorithm between cloud entities based on fuzzy mathematics,''Int. J. Fuzzy Syst., vol. 18, no. 4, pp. 659–672, 2016.
25. Botta A., De Donato W., Persico V., Pescapé A. Integration of cloud computing and internet of things: A survey. Future Gener. Comput. Syst. 2016;56:684–700. doi: 10.1016/j.future.2015.09.021.
26. Tan, J.; Goyal, S.B.; Singh Rajawat, A.; Jan, T.; Azizi, N.; Prasad, M. Anti-Counterfeiting and Traceability Consensus Algorithm Based on Weightage to Contributors in a Food Supply Chain of Industry 4.0. Sustainability 2023, 15, 7855. https://doi.org/10.3390/su15107855
27. Roman R., Lopez J., Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Gener. Comput. Syst. 2018;78:680–698. doi: 10.1016/j.future.2016.11.009.
28. T. Deshmukh, A. Rajawat, S. B. Goyal, J. Kumar and A. Potgantwar, "Analysis of Machine Learning Technique for Crop Selection and Prediction of Crop Cultivation," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 298-311, doi: 10.1109/ICICT57646.2023.10134371.
29. Zhou J., Cao Z., Dong X., Vasilakos A.V. Security and privacy for cloud-based IoT: Challenges. IEEE Commun. Mag. 2017;55:26–33. doi: 10.1109/MCOM.2017.1600363CM.