JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

EDGE COMPUTING SECURITY USING ZERO TRUST EDGE ACCESS

S. Nivetha
Research Scholar, Department of Computer Science and Engineering, Annamalai University, Annamalainagar – 608002, nivethacse555@gmail.com

Dr. R. Saminathan
Associate Professor, Department of Computer Science and Engineering, Annamalai University, Annamalainagar – 608 002, samiaucse@yahoo.com

V. Mahavaishnavi
Research Scholar, Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar – 608 002, vaishnavipriya95@gmail.com

Abstract —Internet of Things (IoT) device proliferation is altering how IT architects upgrade their infrastructures. There is little dispute that data and analysis have advanced to the edge, with a variety of sensors and tracking tools capturing data for practically every imaginable use, from smart cities and energy grids to industries, airlines, automobiles, and retail establishments. In addition to causing service interruptions, new edge computing potential risks such as horizontal assaults, account theft, entitlement fraud, DDoS attacks, and others can also cause other problems. A transformation toward the Zero Trust Security Architecture has been proposed in this work in response to the increase in cyber attacks experienced across these unprotected domains. The difficulties that security teams currently confront can be solved by the confluence of this shift.

Index Terms — Cloud Computing, Edge Computing, Threat detection, Machine learning and Deep learning techniques, Zero Trust Architecture.

I. INTRODUCTION

Recent years have witnessed a surge in Artificial Intelligence (AI) applications and solutions because of deep learning advancements. Millions of Bytes of data are generated at the network edge by the billions of wireless and IoT devices connected to the web as an outcome of the rapid advancements in smart phones and the Machine Intelligence of Things. By 2023, there will be more IP-connected gadgets than people on the planet, more than a threefold increase [1]. Up from 18.4 billion in 2018, there will be 29.3 billion connected gadgets by 2023. Machine-to-Machine (M2M) connections' market share will increase from 33% in 2018 to 50% in 2023 and 14.7 billion M2M connections will exist. The success of IoT and Intelligent systems has intensified the demand to extend the frontiers of AI to the network edge in order to achieve the full potential of big data. Edge Computing is an appealing approach to facilitate computation-intensive intelligent systems at endpoints in order to accomplish this trend. The idea behind edge computing is to gather, store, process, and interpret information close to the point of use in order to accelerate reaction speed as well as conserve bandwidth. Edge

Submitted: 17/10/2022 **Accepted**: 10/11/2022

computing is a distributed data processing system that enables applications to be run closer to information sources such as edge servers, IoT Sensor nodes, and localized endpoints [2]. Therefore, we presume that edge computing could have a similar significant impact on society the way cloud computing had.

Edge computing is different from cloud computing because it could take up to two seconds to deliver messages to a centralized data hub, which leads to delays in the decision-making procedure. Organizations prefer edge computing over cloud computing since the latter can cause shortfalls for them owing to signal latencies. In addition to latencies, edge technology is chosen instead of cloud technology in remote geographical areas with poor or nonexistent access to a centralized site. Edge computing offers the ideal solution for this local storage requirement, which is analogous to that of a miniature data centre, at these locations shown in figure 1. Cloud and edge computing can coexist. The edge extends and enhances the cloud. The following are the primary benefits of fusing cloud and edge computing [3]:

- Performance of the backhaul: Autonomous edge computing nodes are capable of handling a variety of calculation activities without transferring the underlying data to the cloud.
- Accelerated service response: Deployed edge-based intelligent applications can dramatically speed up reaction times and cut down on transmission delays.
- Robust cloud backup: The cloud can offer strong processing power and vast, scalable storage in circumstances where the edge cannot afford it.

The edge devices, edge servers, edge networks, and core infrastructure can be seen as the four functional layers that comprise the model of edge computing [4][5]. These layers accomplish the following tasks:

a) Edge Devices (end users): The edge network contains many linked devices that serve as data producers and consumers, such as Internet of Things (IoT) devices.

b) Edge Network: The World Wide Web (WWW), data centre networks, and wireless communication networks connect the whole infrastructure, encompassing servers, devices, and core infrastructure.

c) Edge Servers: These servers, which are owned and supplied by infrastructure providers, are in charge of supplying virtualized management services. Additionally, edge data centers that are linked to the conventional cloud are being established.

d) Core Network: The core network is responsible for providing network access, notably internet, wireless, and cloud computing services.

EDGE COMPUTING: TO THE CORE

A. Security Vulnerabilities common to Edge Computing

In many ways, edge computing is a type of minimized data centre. Minimization can frequently imply that security elements are removed or scaled back to reduce the cost of the edge facility

[6]. Although it's not the only factor, this is the main incremental security risk source in edge computing. Other factors include:

- Information backup, collection, and safeguards vulnerabilities: As already been mentioned, data kept at the edge is not often subject to the same physical security measures as data centers. In reality, it might be easy to copy data from a memory stick or remove the disc from an edge computing resource and seize a whole database. It may be challenging or even impossible to back up crucial files in edge computing facilities due to their restricted internal storage possibilities, which means that in the event of an incident, there might be no replicate copy to rescue the databases.

- Threats from passwords and authentication: Edge data centers are seldom backed by native, security-conscious IT personnel. This situation encourages weak password practices, such as admitting default credentials, using simple common passwords to memorize, publishing notes with passwords for specific systems, and failing to change passwords frequently. In many cases, maintaining the edge systems may be a part-time job assigned to many people. Similarly, for the convenience of both users and administrators, edge systems may refrain from employing robust authentication techniques like multifactor / two-stage verification.

- Challenges of perimeter defence: Edge computing makes perimeter defence more challenging and widens the IT periphery. The credentials for this are frequently saved at the edge since edge systems themselves may need to authorize their apps with collaborator apps in the data centre. This implies that a compromise in edge security may reveal authentication information for data centre assets, greatly extending the scope of the security incident.

- Risks of cloud migration: Different cloud software platforms and services approach edge aspects in different ways, it can be simple to lose track of the specific link between edge and cloud. Giving edge devices a secure access to cloud resources and apps can be challenging if they are basic controllers, which is frequently the case. Because of this, it is particularly critical to evaluate access control, cloud-to-edge connectivity, and other security measures.

- IoT and edge security threats: IoT edge applications provide significant security holes. Since IoT devices are built for minimal cost, low power dissipation, and deployment in environments that are frequently not suited for complicated technology due to factors like temperature and humidity, dust, or vibration.

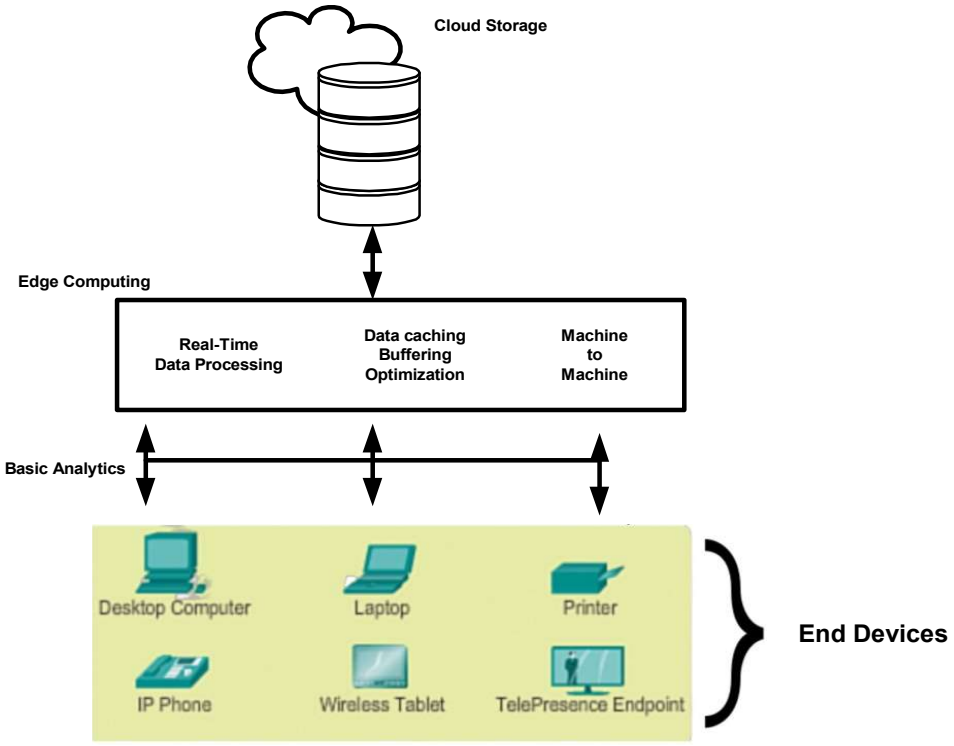


Figure 1 Edge Computing Paradigm

B. Edge Intelligence

Edge intelligence refers to a network of interconnected systems and peripherals that use AI systems to gather, cache, interpret, and analyze data near the location of data acquisition. Edge intelligence strives to improve data processing while preserving user and data security and privacy. The crucial distinction between edge intelligence and conventional approaches is with edge intelligence, processing of data and applications is conducted locally on the sensor rather than exporting all data to a particular remote server [7]. Edge caching, edge training, edge inference, and edge offloading are the first four key elements of edge intelligence that uncovers [8].

In edge intelligence, data created by edge devices is gathered and stored using a distributed storage system named edge caching. For instance, there are a lot of comparable pixels among subsequent frames in prolonged mobile visual field analysis. Certain edge nodes with limited resources must transmit gathered footage to edge services or the cloud for additional processing. With cache, edge devices merely need to upload various pixels or frames. Based on the training set cached at the edge, the hidden patterns, or the best values for all the biases and weights are gained while training. Typically, edge servers or end devices are used for edge learning. Meanwhile, compared to training on a processor or a GPU, training is substantially slower. In order to compute the output on edge systems and servers, algorithms are employed

to infer the testing entity in a forward pass. Offloading techniques that manage the distribution of processing power among the various tasks are used in conjunction with inference and training techniques. With the existence of billions of devices and an increase in 5G users, edge devices would therefore emerge.

C. Zero Trust Security Framework

Zero Trust is a security framework that mandates that before granting or maintaining access to applications and data, all users whether inside or outside the organization's network must first authenticate, authorize, and undergo ongoing security configurations and posture validation. The strategy of "never trust, always verify" is the foundation of the zero-trust approach [9]. In parallel, before granting access, the system must verify each and every entity that requests a connection to its resources, each and every time the user attempts to interact with the system, thus asserting that all network traffic should be regarded as untrusted [10]. It refers to a security threat model without the assumption that the users, devices, data, applications, and services that operate within the security limit of an organization should be automatically trusted.

Therefore, trust architecture necessitates businesses to frequently check and verify that a customer and their device have the proper permissions and credentials. Together with compliance or other requirements to take into account before approving the transaction, it also necessitates the implementation of a policy that takes customer and device risk into account. In order to set controls on what and where they connect, it is necessary for the organization to be aware of all of its services and premium profiles. Onetime validation seems insufficient since threats and consumer characteristics are all dynamic [11]. The underlying factors assist to implement a zero-trust approach in a cloud and edge integrated computing environment [12]:

(i)Determination of Sensitive Data: This is the basic notion behind the Zero Trust concept. To choose the appropriate security, the edge service provider must identify critical information, such as personal details, health records, proprietary information, or credit and debit card data. Additionally, this notion supports the idea that the system design of edge deployment guarantees proper security of the critical data [31].

(ii)Routing Sensitive Information Flows: This aspect relates to tracking the movement of private information over the edge network. This concept results in the formation of micro-networks as this flow may be multidirectional [32-34].

(iii)Later part Authorization (People): The Zero Trust strategy is based on the authentication of trusted users and identification security. Technologies like Identity and Access Management (IAM), Multi-Factor Authentication (MFA), etc. are included in this. Because of this, all permissions are constantly monitored and verified for user credibility.

(iv)Machine Authorization: The most important and fundamental aspect of a Zero Trust approach is machine trustworthiness. Therefore, mechanism of record solutions like Device Managers must be used to evaluate the machines or devices connected to the edge.

(v)Limiting Accessibility: The least privileged access rights describe Zero Trust protection. The importance of access control has increased for edge security. Additionally, excessive access

that results in insider incidents is the primary cause of insider threats in the cloud computing paradigm.

(vi)Application Security: Adoption of Application Security Zero Trust focuses on protecting and managing the application layer, along with containers and virtual machines. In the Zero Trust method, Multi-Factor Authentication (MFA) has been regarded as enabling the appropriate access control to applications.

(vii)Analyze the ecosystem of zero trust with security analytics: Through the use of logging and data analytics, the entire micro perimeter ecosystem will be scanned for any harmful activities. Additionally, Zero-Trust makes use of a variety of analytical system capabilities, including advanced security analytics and security user behavior analytics, to enable edge security specialists to monitor what is occurring at any given moment and deploy defences more wisely.

Several researches relating to data collecting security is currently being conducted. There are two groups into which the studies have been grouped. Targeted defending tactics comprise the first category. The strategy's major goal is to respond appropriately to attacks based on the traits of malicious node attacks, thereby nullifying the attack. A Security and Energy Efficient Disjoint Route (SEDR) technique countering the black attack, for instance, was proposed by Liu et.al. [13] The other type of prevention is a strategy that can be used in most scenarios. A trust-based strategy is the most effective way to ward off attacks [14]–[16]. Instead of adopting a targeted attack action, this sort of method adopts the appropriate data routing technique to determine the node's trust level. The node is seen as trustworthy and its trust is increased if its behavior matches what is expected of it [29][30]. If not, its credibility is diminished. When a node transmits data, a high-trust node is chosen as the intermediary node to minimize the selection of malicious nodes, which can enhance the likelihood that the data will be successfully communicated.

D. Network Edge Machine Intelligence Techniques

The current advances in Artificial Intelligence (AI) and the enormous volume of data make deep learning technology advisable. The driving factor for moving learning to the edge is to enable quick access to the massive amounts of real-world data produced by network edge for rapid AI model training and interpretation, which in turn gives the devices humanlike intellect to react quickly to actual events [17]. Deep learning algorithms often demand enormous amounts of data and processing power. Real-time data sources include limited power IoT devices like standard cameras. However, they are inappropriate for the training and inference of deep learning models due to their constrained computing and storage capacities [5]. By fusing deep learning with edge computing, edge AI technology offers a remedy. Consequently, edge devices or servers are positioned close to those end devices and used for installing deep learning models that employ IoT-generated data. Deep learning calculations are anticipated to be moved as much as feasible from the cloud to the edge thanks to edge intelligence. This makes it possible to create a range of decentralized, low-latency, durable, and intelligence services. One of the most significant developments in Machine Learning (ML) edge computing

is the need for real-time processing in Computer Vision (CV) applications that deal with large amounts of data, like video pictures and Natural Language Processing (NLP).

E. Contributions of the Work

The following contributions are produced through this study:

- Outlining trust management problems at the edge of the edge computing network architecture, providing a rigorous analysis of the methods and approaches that have already been proposed to address trust management problems.
- Putting out a cutting-edge trust management system to guarantee data security at the edge and strong trust relying on edge devices for quick and effective communication and processing.

II. LITERATURE REVIEW

In order to serve edge computing, Yuan and Li [18] developed a trust model that may also be applied to larger-scale computing. Their inter-feedback approach introduced three primary layers: the network, the broker, and the device layer, and embraced the concept of Global Trust Degree (GTD), which is direct trust and feedback trust from brokers and edge nodes. The term "multisource" refers to the generation of feedback from both edge devices and service brokers. For the efficiency assessment, Global Convergence Time (GCT) was used. Using the NetLogo event simulator and a Personalized Similarity Measure (PSM) experiments were done. Using the Task Failure Ratio (TFR), reliability was evaluated.

The provision of configuration updates, control commands, and the sending and receiving of status data is a constant requirement for providers of smart services. In that same context, Industrial IoT (IIoT) controllers must assure the accuracy of inputs and safeguard themselves against unwanted interference. [19] Demonstration of a trust mechanism for edge devices in an Industrial IoT (IIoT) setting addressed this issue by demonstrating how to achieve confidentiality, reliability, and validity at both the software and hardware domains. A Trusted Execution Environment (TEE) was crafted in a slightly updated Real-Time Operating System since Trust Zone is receiving a lot of attention as a result of Advanced RISC Machine (ARM) processors; however, no additional implementation was available.

An IoT trust domain [20] to safeguard IoT environment from harmful threats with a reliable gateway solution was suggested. Smart workplaces and home automation both could be benefited from this approach. The solution moves IP addresses through a gateway system, where they were later changed to IDs. All connected devices' ID info was kept in a network's ID table, which served as a repository. Although no implementation was offered, theoretically the system performed well when compared to an untrusted domain. A methodology presented by Mendoza and Kleinschmidt [21] detected faulty nodes based on the services they selected to offer. All nodes initially had a trust value of 0 and notification packets were sent to initiate the neighbor finding process. A node's trust value increased when it rendered a service, and it reduced when it failed to do so. The implementation of this trust mechanism in the Cooja simulation made available by Contiki OS resulted in the successful detection of rogue nodes.

Nodes exchange credentials for third-party intrusion-related verification in order to communicate. Even so, access is restricted in a tactical context, such as during military activities or search and rescue missions. Furthermore, it is impossible to distribute passwords early on or guarantee hardware stability. To address these issues, [22] suggested a paradigm using strategic cloud resources that provide data staging, screening, onward deployment, and data-gathering points for disjointed systems. Identity-Based Cryptography (IBC), OpenSSL ciphers, and Stanford Identity-Based Encryption (IBE) are used in the recommended trust approach. A threat model created by Microsoft Security Development Lifecycle (SDL) is utilized to assess the system. Of the 60 potential risks it suggests, 14 are taken into account for the strategic environment. 12 out of 14 threats were completely and partially handled after deployment utilizing open-source strategic cloud resources.

More than half of IoT devices are smart phones connected to wireless networks, and these devices are open to several security risks. [23] Focused on a Model for Data Privacy and provided a trust management framework for the application, communication, and sensor layers-the three levels that make up the IoT architecture. The architecture was centered on a security specialist with ample processor and memory power to handle all operations, reducing overload for devices with limited resources [26-28]. Among the methods utilized by the system for authentication were the elliptic curve cryptosystem, context-aware location privacy, the zero-knowledge protocol, mechanisms for access control, and the distribution of public keys by the security manager. Additionally, layer encryption techniques and data origin authentication schemes were used for packet security and anonymity. The concept was straightforward and addressed every issue; however, there was no appropriate examination or demonstration. Further, the security administrator, whose failure would bring down the entire system, performed more than half of the processing.

A general trust management approach for IoT infrastructure was put forth by Sharma et al. [24]. It outlined all specifications needed to determine whether edge devices can be trusted with updates and services. To assess the system, a novel trust or and trustee idea was taken into account. The system as a whole has four phases: In order to compute trust, models such as machine learning, flow, fuzzy, probabilistic, and statistical models were used. Two architectures, centralized and distributed, were used for trust dissemination. The final phase included update and maintenance, which took place in an event-driven and time-driven circumstance. There was no suitable implementation provided as it is a generic framework.

III. PROPOSED ZERO TRUST SECURITY ARCHITECTURE FOR EDGE AI

By eliminating unauthorized users and unmanaged devices and restricting all lateral movement, the Zero Trust security framework helps to secure on-premises as well as edge/cloud resources. Crypto algorithms, device authentication, Identity and Access Management (IAM) and multifactor identity management are among the technologies that Zero Trust uses [25]. Additionally, applying this paradigm necessitates the validation and reliability testing of all network related and external components. Likewise, the principle of minimal access is upheld

when permission is granted through this security model, and the user is restricted to only those resources that are permitted for each and every user.

The Microcore and Perimeter

To safeguard the network and its data, modern networks rely on a variety of security tools and measures. These consist of firewalls, Intrusion Prevention Systems (IPS), gateways for content filtering and Virtual Private Networks (VPN), as well as other encryption tools. [26] Anticipates the creation of a brand-new product category termed a network Segmentation Gateway (SG) for this future-state network. This incorporates all of the characteristics and capabilities of distinct, discrete security solutions into the very structure of the SG. Designers have a device that can be placed right in the middle of the network because of the inclusion of a packet-forwarding engine. The greater value of the SG is in its capacity to securely segment networks appropriately and incorporate security into the fundamental infrastructure of the network.

A segmentation gateway would need numerous high-speed links and specific global policy. This integrates security into the structure of the segmentation gateway. Each switching zone connected to an interface in the Zero Trust network is referred to as a "Microcore and Perimeter" (MCAP) is shown in figure 2. Due to the shared functionality and global policy attributes of all the resources inside a given microcore, each segmented zone functions as its own microcore switch and can be thought of each zone as a micro perimeter. By combining all the switches found within all the MCAPs into a single switching mesh, you can centrally manage all MCAP.

The evaluation of nodes' trust is the central concept of this research. Higher trust is assigned to nodes who faithfully carry out their mandate, while lower trust is assigned to nodes that behave unpredictably, preventing low-trust nodes from taking part in the data collecting process [27][28]. A node's overall trust level is calculated by integrating its trust level across the most recent time. The average value of trust degree evaluation is the most basic way of synthesizing trust level. The overall proposed framework is depicted in Figure 3. Figure 3 shows the architecture and the workflow automation goes from the total request to access control and its validation. Once the validation is done the access get transfers to the appropriate assets.

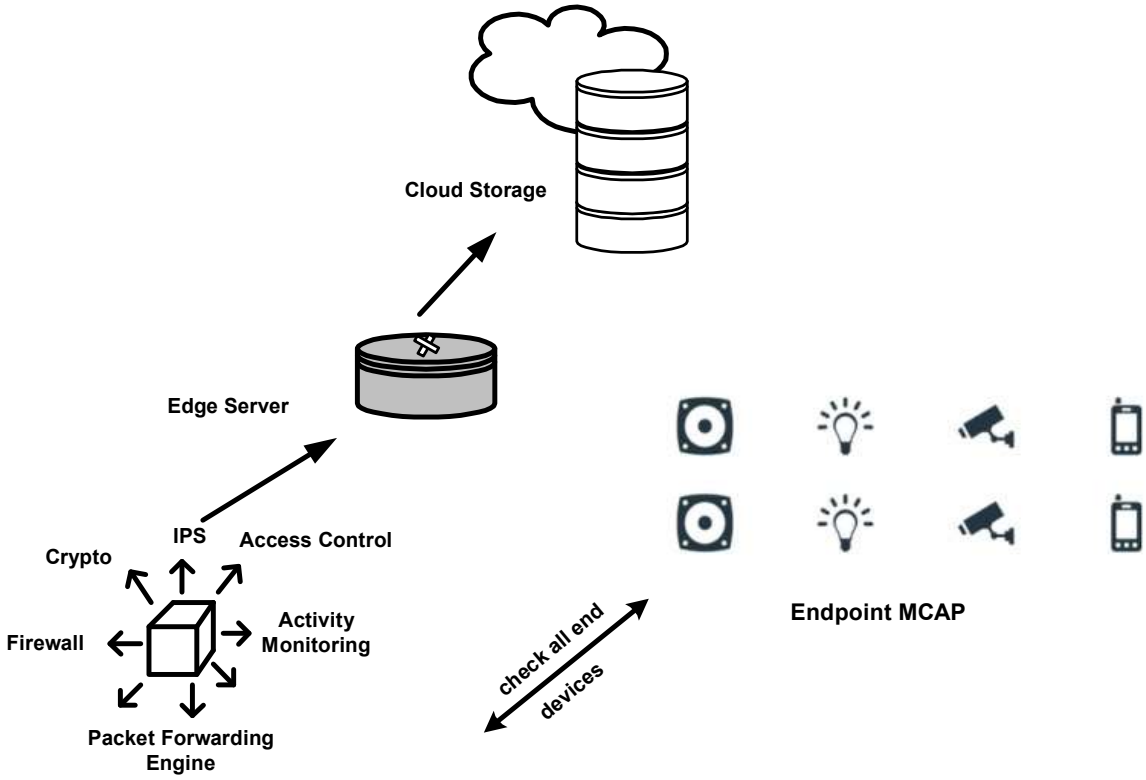


Figure 2 Microcore and Perimeter

The preceding is the typical approach for evaluating trust:

Mobile edge nodes first gather the sensor nodes' trust information, which they then analyze to determine the value of the trust chains. Then, mobile edge nodes update storage by uploading the trust values, including base stations and ground receivers. Finally, edge devices like base stations will upload pertinent results if there are cloud mandates. The algorithm [27] for trust evaluation is as shown below:

For Node A Do

Assign an initial value trust value $\Phi$of a node A and the degree of change Φ' of the trust value

if *nodeAistrusted* then $\Phi=\Phi+(\Phi-\Phi')$

else$\Phi=\Phi-(\Phi-\Phi')$

if Φ value is greater than the threshold value then node is trusted

else not trusted

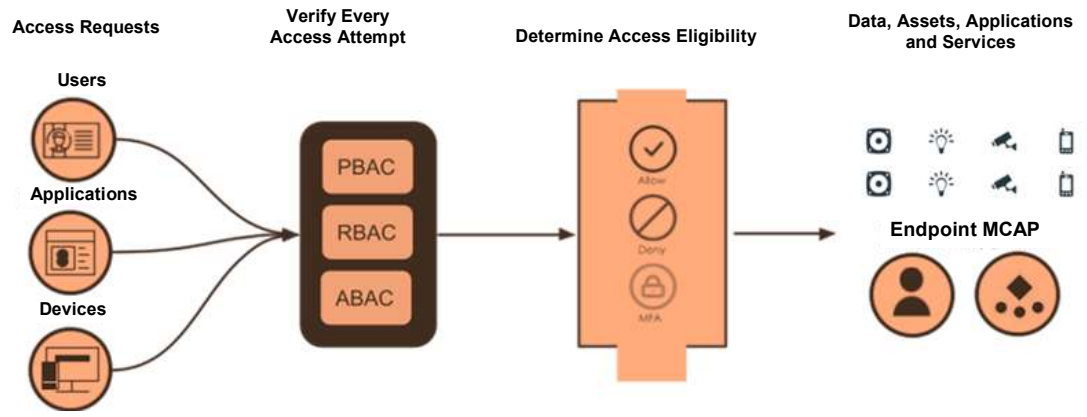


Figure 3 The proposed framework

IV. EXPERIMENTAL SETUP

Due to the cost effective feature of edge computing, more numbers of large scale, small and medium scale enterprises universally adopt it. The edge environment is created using a secure network running in Edge Core Switch. 5 computers were added out of which 2 runs in Ubuntu, 1 in Windows 11, 1 in Kali Linux and 1 runs Windows server 2022, data centre version. Kali Linux machine is used as attacker machine and rest all are the clients connected to the server. All the traffic are captured and interpreted by the server machine. For security purpose all the IPs are masked and the entire network remain anonymous.

V. RESULTS AND DISCUSSION

The entire experimentation is carried out to ensure the reliability of zero trust edge access to the nodes under the experimental setup is shown in figure 3. In order to ensure the privacy part of experimentation, all the IP addresses were anonymized. This creates a more challenge to validate the proposed claim. In addition, to ensure zero trust, the attacker machines identities were also masked so that it can look legitimate. The traffic flow monitoring is enabled for all the interfaces. Traffic overview and its representation: TS → Time Stamp, pp → port/protocol, class denotes the ground truth mention of the IP. Further, the results are statistically analyzed and validated with different distribution function such as Cumulative Distribution Function (CDF) and Empirical CDF (ECDF) etc. Dataset which we considered were collected in the public honeypot (TPOT based honeypot project deployed in the cloud) between the dates March 2020 – March 2022. Figure4 – Figure8 shows the output results of the proposed claim. Figure 4 shows the total IP activities against the total ports in the communication protocol stack. Figure 5 and 6 shows the statistical report of the total volumetric data where Figure 7 shows the unique IP statistics and the pattern.

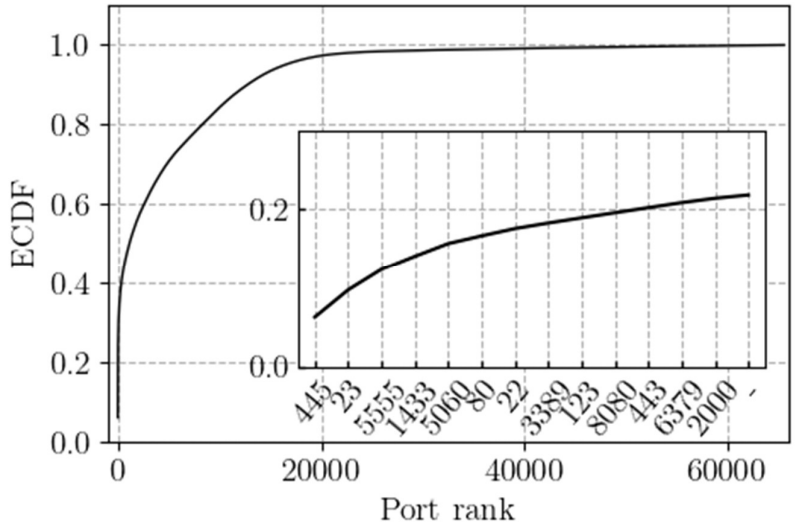
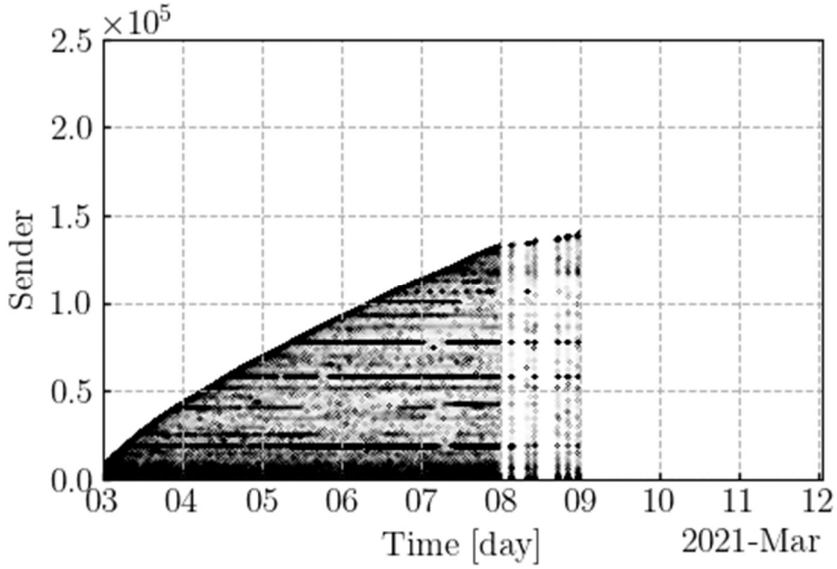
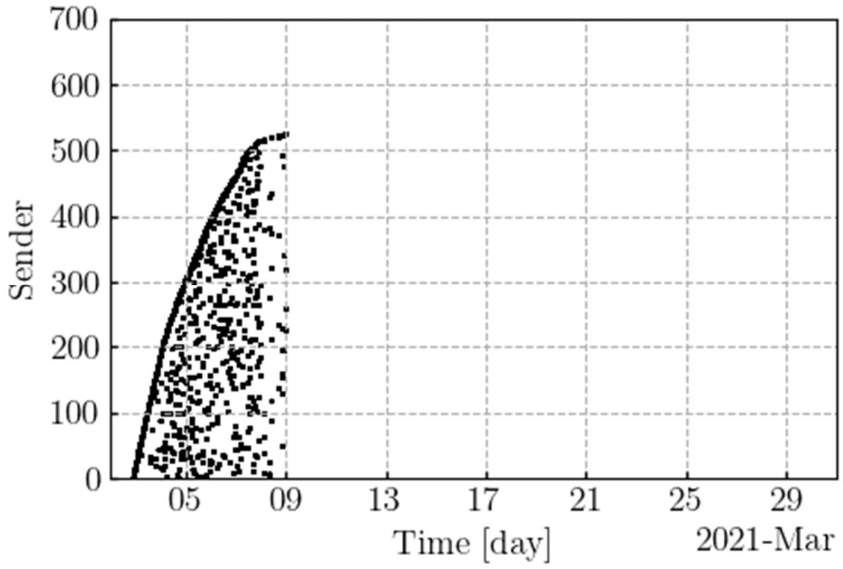


Figure 4 IPs activity pattern along with probabilistic ECDF vs port rank



(a) Data volume (per day)



(b) Data volume (per 4 days)

Figure 5 Statistics of the total volumetric data

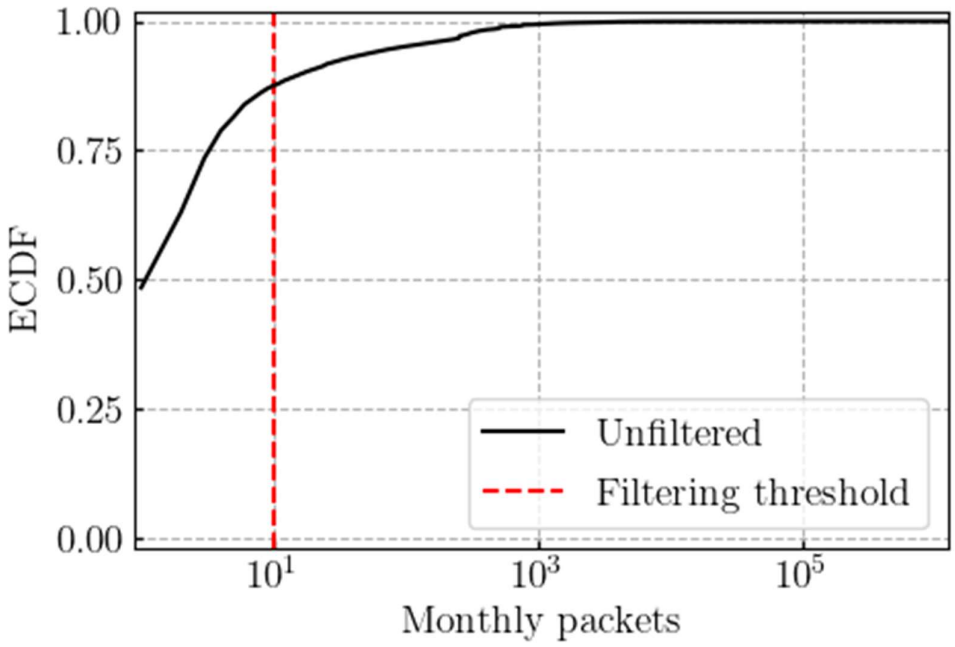


Figure 6 Statistics of the total volume/month (random data: March 2021)

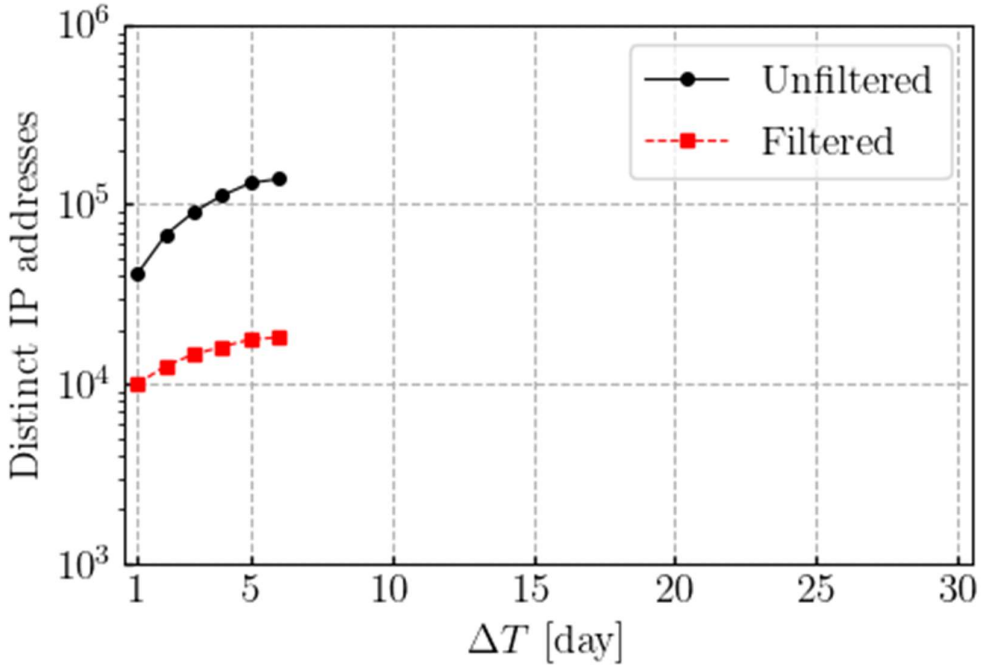


Figure 7 Statistics of unique IP and its traffic pattern (24/7/365)

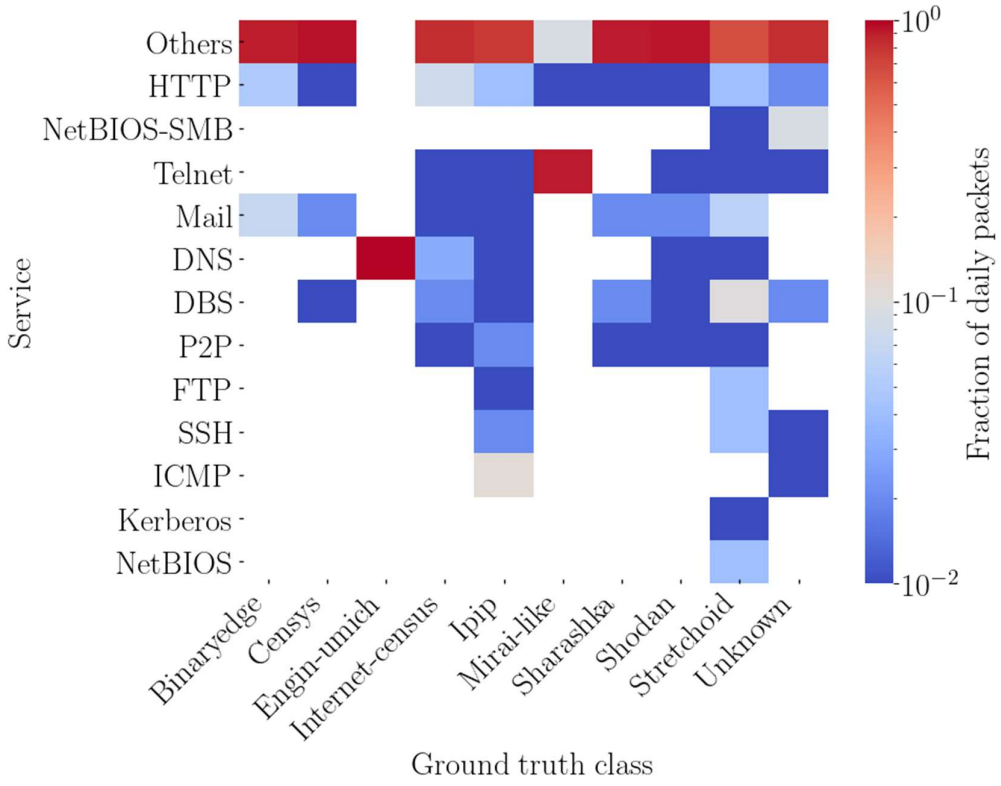


Figure 8 Confusion Matrix of the ports/protocols

From the experimental results as depicted in the graphs shown in the Figure 4 – figure 8, it is very clear that the proposed model is efficient enough to classify the data pattern among the nodes within the network. Figure 8 shows the confusion matrix generated for the ground truth class and total service available for classification. This achieves the higher layer of security with zero trust knowledge towards knowing the data flow in the network. Even the infected computer data is classified anonymously.

VI. CONCLUSION

In edge computing, as we perceive that as well, data collection, transmission, retention, and computation all take place at the network's edge. Edge computing also addresses a significant issue with bandwidth in cloud computing, but new issues including privacy, security, latency, computation power at the edge, and offloading need to be addressed. The establishment of the trust is one of the numerous issues that edge computing confronts. By offering a trust management approach to assess the dependability of edge nodes, this research aims to address the most important problem relating to the security and reliability of edge devices.

REFERENCES

[1]"Cisco Annual Internet Report (2018–2023) White Paper," [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.html, Accessed: 2021-08-03.

[2]N. Moustafa, K.-K. R. Choo, and A. M. Abu-Mahfouz, "Guest editorial: AI-enabled threat intelligence and hunting micro services for distributed industrial IoT system," IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 1892–1895, 2022.

[3]D. Balouek-Thomert, E. G. Renart, A. R. Zamani, A. Simonet, and M. Parashar, "Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows," The International Journal of High Performance Computing Applications, vol. 33, no. 6, pp. 1159–1174, 2019.

[4]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. 18209–18237, 2018.

[5]M. S. Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan, and F. Hussain, "Machine learning at the network edge: A survey," ACM Computing Surveys (CSUR), vol. 54, no. 8, pp. 1–37, 2021.

[6]J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," Future Generation Computer Systems, vol. 89, pp. 525–538, 2018.

[7]H. HaddadPajouh, R. Khayami, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "Ai4safe-iot: An ai-powered secure architecture for edge layer of internet of things," Neural Computing and Applications, vol. 32, no. 20, pp. 16119–16133, 2020.

[8]D. Xu, T. Li, Y. Li, X. Su, S. Tarkoma, T. Jiang, J. Crowcroft, and P. Hui, “Edge intelligence: Empowering intelligence to the edge of network,” Proceedings of the IEEE, vol. 109, no. 11, pp. 1778–1837, 2021.

[9]Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, “Protection of sensitive data in zero trust model,” in Proceedings of the International Conference on Computing Advancements, 2020, pp. 1–5.

[10]T. Wang, P. Wang, S. Cai, X. Zheng, Y. Ma, W. Jia, and G. Wang, “Mobile edge-enabled trust evaluation for the internet of things,” Information Fusion, vol. 75, pp. 90–100, 2021.

[11]C. Buck, C. Olenberger, A. Schweizer, F. Volter, and T. Eymann, “Never¨ trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust,” Computers & Security, vol. 110, p. 102436, 2021.

[12]Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, “A survey on zero trust architecture: Challenges and future trends,” Wireless Communications and Mobile Computing, vol. 2022.

[13]Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, “Secure and energy efficient disjoint multipath routing for wsns,” IEEE Transactions on Vehicular Technology, vol. 61, no. 7, pp. 3255–3265, 2012.

[14]D. Arivudainambi, K.A. Varun Kumar, S. Sibi Chakkaravarthy, P. Visu, “Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance”, Computer Communications, Vol.147, November, 2019, pp.50-57, Elsevier.

[15]T. Wang, P. Wang, S. Cai, Y. Ma, A. Liu, and M. Xie, “A unified trustworthy environment establishment based on edge computing in industrial IoT,” IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6083–6091, 2019.

[16]Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, “A trust-based minimum cost and quality aware data collection scheme in p2p network,” Peer-to-Peer Networking and Applications, vol. 13, no. 6, pp. 2300– 2323, 2020.

[17]L. Morra, F. Lamberti, F. G. Prattico, S. La Rosa, and P. Montuschi,´ “Building trust in autonomous vehicles: Role of virtual reality driving simulators in HMI design,” IEEE Transactions on Vehicular Technology, vol. 68, no. 10, pp. 9438–9450, 2019.

[18]M. Merenda, C. Porcaro, and D. Iero, “Edge machine learning for AI enabled IoT devices: A review,” Sensors, vol. 20, no. 9, p. 2533, 2020.

[19]S. Sibi Chakkaravarthy, V. Vaidehi and Steven Walczak, “Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles", Journal of Medical Systems, Vol.44, Article 29, Springer.

[20]J. Yuan and X. Li, “A multi-source feedback based trust calculation mechanism for edge computing,” in IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2018, pp. 819–824.

[21]S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, “IoTeed: An enhanced, trusted execution environment for industrial IoT edge devices,” IEEE Internet Computing, vol. 21, no. 1, pp. 40–47, 2017.

[22]E. Kim and C. Keum, “Trustworthy gateway system providing IoT trust domain of smart home,” in 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2017, pp. 551–553.

[23]C. V. Mendoza and J. H. Kleinschmidt, “Defense for selective attacks in the iot with a distributed trust management scheme,” in 2016 IEEE International Symposium on Consumer Electronics (ISCE). IEEE, 2016, pp. 53–54.

[24]Dedipyaman Das, S.Sibi Chakkaravarthy, Suresh Chandra Satapathy, “A Decentralized Open Web Cryptographic Standard”, Computers and Electrical Engineering, Elsevier, Vol. 99, 107751, April, 2022.

[25]S. Echeverr´ıa, D. Klinedinst, K. Williams, and G. A. Lewis, “Establishing trusted identities in disconnected edge environments,” in 2016 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, 2016, pp.51–63.

[26]K. R. Rehiman and S. Veni, “A trust management model for sensor enabled mobile devices in IoT,” in 2017 International Conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017, pp. 807–810.

[27]S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi,“A Survey on malware analysis and mitigation techniques”, Computer Science Review, Vol. 32, pp 1 - 23, May 2019, Elsevier.

[28]Sharma, E. S. Pilli, A. P. Mazumdar, and M. Govil, “A framework to manage trust in internet of things,” in 2016 International Conference on Emerging Trends in Communication Technologies (ETCT). IEEE, 2016, pp. 1–5.

[29]S. Sibi Chakkaravarthy, Pranav Kompally, Saraju P Mohanty and Uma Chopalli,“MyWear: A Novel Smart Garment for Automatic Continuous Vital Monitoring”, IEEE Transactions on Consumer Electronics, IEEE, Vol. 67, No. 3, pp. 214-222, 2021.

[30]Kerman, O. Borchert, S. Rose, and A. Tan, “Implementing zero trust architecture,” National Institute of Standards and Technology, vol. 2020, pp. 17–17, 2020.

[31]J. Kindervaget al., “Build security into your network’s DNA: The zero trust network architecture,” Forrester Research Inc, vol. 27, 2010.

[32]Sangeetha D, S. Sibi Chakkaravarthy, Suresh Chandra Satapathy, Vaidehi V and Meenaloshini Vimal Cruz,“Multi Keyword Searchable Attribute Based Encryption for efficient retrieval of Health Records in Cloud”, Multimedia Tools and Applications, Springer, 2021.

[33]W. Mo, T. Wang, S. Zhang, and J. Zhang, “An active and verifiable trust evaluation approach for edge computing,” Journal of Cloud Computing, vol. 9, no. 1, pp. 1–19, 2020.

[34]Y. Liu, M. Dong, K. Ota, and A. Liu, “Active trust: Secure and trustable routing in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013–2027, 2016.