NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE (AUTONOMOUS)

Pampady, Thiruvilwamala, Thrissur, Kerala-680 567
NAAC 'A' Accredited, Approved by AICTE-New Delhi
Affiliated to APJ Abdul Kalam Technological University, Kerala
An ISO 9001:2015 Certified Institution

DEPARTMENT OF MCA

SEMINAR REPORT

ON

SECURITY IMPACTS OF EDGE COMPUTING ON CLOUD INFRASTRUCTURE

Submitted by

PRANAV SUNNY

(NCE23MCA-2042)

Under the guidance of

Ms. SUMI M, MCA
Assistant Professor

Department of MCA,NCERC,Pampady ,Thrissur

MARCH 2025

SEMINAR REPORT

ON

SECURITY IMPACTS OF EDGE COMPUTING ON CLOUD INFRASTRUCTURE

Submitted in partial fulfillment of the requirement for the award of degree in

MASTER OF COMPUTER APPLICATIONS

OF THE

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Submitted by

PRANAV SUNNY

(NCE23MCA-2042)

Under the guidance of

Ms.SUMI M , MCA
Assistant Professor

NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE,

PAMPADY, THIRUVILWAMALA, THRISSUR-680567

MARCH 2025

NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE

DEPARTMENT OF MCA

COLLEGE VISION

To mould true citizens who are millennium leaders and catalysts of change through excellence in education.

COLLEGE MISSION

NCERC is committed to transform itself into a center of excellence in Learning and Research in Engineering andFrontier Technology and to impart quality education to mould technically competent citizens with moral integrity, social commitment and ethical values. We intend to facilitate our students to assimilate the latest technological know-how and to imbibe discipline, culture and spiritually,and to mould them in to technological giants, dedicated research scientists and intellectual leaders of the country who can spread the beams of lightand happiness among the poor and the underprivileged.

DEPARTMENT VISION

To create a school of distinction for the PG students, prepare them to be industry- ready, and achieve Academic excellence by continuous endorsement of the faculty team in terms of Academics, Applications & Research.

DEPARTMENT MISSION

The Department of Computer Applications strives to provide quality and competency-based education and fine-tune the younger generation through Curricular, Co-Curricular and Extra-curricular activities so as to encounter theProfessional and Personnel challenges ahead with Pragmatic skills & courage, thereby ‘Creating thetruecitizens.

NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE, PAMPADY

CERTIFICATE

This is to certify that the seminar entitled “**SECURITY IMPACTS OF EDGE COMPUTING ON CLOUD ARCHITECTURE**” submitted in partial fulfillment of the requirement for the award of the degree of Master of Computer Application of the University of KTU is a result of bonafide work carried out by **“PRANAV SUNNY”** of batch 2023-25 in the Department of MCA under the guidance of **Ms.SUMI M**, Assistant Professor, Department of MCA, NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE, PAMPADY under my supervision and guidance.

Guide **Head of the Department**

Principal **External Examiner**

DECLARATION

I hereby declare that the seminar report entitled "**SECURITY IMPACTS OF EDGE COMPUTING ON CLOUD ARCHITECTURE"** submitted to the **MCA DEPARTMENT** of **NCERC** in partial fulfillment of the requirement for the award of degree in **MASTER OF COMPUTER APPLICATION** from **KTU,** a record of original work done by me under the guidance of **Ms. Sumi M**, Assistant Professor of MCA department, during Fourth Semester MCA course period.

PLACE **PRANAV SUNNY**

DATE

ACKNOWLEDGMENT

First and most, I thank the **God Almighty** for showing me the path to the completion of seminar work.I thank **Prof. DR K G VISWANADHAN**, the principal of **NCERC**, for providing a good atmosphere for seminar completion and presentation. I thank **Dr. Sudheer S Marar** ,Head of the MCA Department, and my seminar co-ordinator **Ms.SUMI M**, Assistant Professor of the MCA Department, and my seminar coordinator for the guidance and support. I express my immense gratitude to all my friends, without whom I would have never been able to do my seminar well.

CONTENTS

1. INTRODUCTION

Edge computing represents a decentralized information technology framework where data processing occurs at the periphery of the network—close to the source where the data is initially produced. In today's digital era, data is regarded as a critical asset, delivering valuable insights and playing a pivotal role in facilitating informed decision- making to ensure seamless business operations. Effectively managing the influx of data requires robust systems capable of safeguarding information from unauthorized access while enabling real-time operations across multiple devices and geographic locations. The integration of traditional cloud computing architectures often poses challenges in handling data flow efficiently. This limitation underscores the necessity of incorporating edge computing into cloud networks to streamline information processing. By processing and analyzing data at its point of origin, edge computing reduces latency and eliminates the need to transmit raw data to centralized data center.Data and resource security remain paramount across industries, and edge computing is no exception. Ensuring secure data exchanges between interconnected devices and users necessitates deploying advanced tools and methodologies for vulnerability management, intrusion detection, and threat mitigation. Security measures must also extend to IoT devices and sensors, as these endpoints are susceptible to unauthorized intrusions and cyberattacks. Other potential security concerns involve data storage vulnerabilities, perimeter defenses, authentication protocols, physical breaches, and malicious hardware or software injections. This study conducts a comprehensive review of prior research to explore the security implications of edge computing in cloud networks, offering deeper insights into addressing these challenges.

2. LITERATURE REVIEW

Tabrizchi, H., and Kuchaki Rafsanjani,[1] M.study (2020) presented a comprehensive review of cloud computing security concerns, categorizing them as threats, vulnerabilities, and solutions. They identify vulnerabilities such as data breaches, DDoS assaults, insider threats, and APTs, underlining the hazards associated with shared and distributed cloud infrastructures. The study also highlights risks due to multi-tenancy, virtualization, and API mismanagement, which are compounded by dependency on third-party services. To reduce these threats, the authors recommend encryption, strong authentication, virtualization security improvements, and compliance frameworks. They also push for research into new technologies such as blockchain and AI to improve cloud security and encourage stakeholder engagement to create a secure ecosystem.

Abdulsalam, Y.S., and Hedabou, M[2]. (2021) provided a technical assessment of security and privacy challenges in cloud computing. The study divides these difficulties into three major categories: data security, privacy preservation, and compliance. They cover concerns such as illegal access, data breaches, and privacy violations caused by the multi-tenant structure of cloud services. The authors also point out weaknesses in cloud systems caused by insufficient access controls, weak encryption protocols, and misconfigurations. To overcome these challenges, they suggest using advanced encryption techniques, privacy-preserving mechanisms such as homomorphic encryption and differential privacy, and strong identification and access management systems. The evaluation underlines the necessity of compliance with legislative frameworks and industry standards for safeguarding sensitive data in cloud settings.

Cao .,[3] (2020) conducted a comprehensive review of edge computing research, highlighting its benefits, limitations, and technological breakthroughs. Edge computing is a distributed computing system that processes data at or near its source, lowering latency and bandwidth utilization. The study underlines the necessity of real-time data processing in applications such as driverless vehicles, healthcare monitoring, and industrial automation. Edge computing improves performance and reliability by reducing the amount of data transmitted to central servers. The study also defines the fundamental components of edge computing, such as edge devices, edge servers, and communication networks, and explores several architectural approaches.

Parast . [4](2022) conducted an assessment of cloud computing security in service-based models, emphasizing the importance of addressing security vulnerabilities in cloud environments. It divides cloud services into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each having unique security requirements and risks. The study emphasizes major difficulties such as maintaining data confidentiality, integrity, and availability while limiting risks such as multitenancy and illegal access. The study examines security techniques such as encryption, access control, and intrusion detection, as well as upcoming technologies like blockchain, machine learning, and zero-trust architectures. It provides insights into specialized security solutions for each service model and serves as a comprehensive reference for improving cloud security.

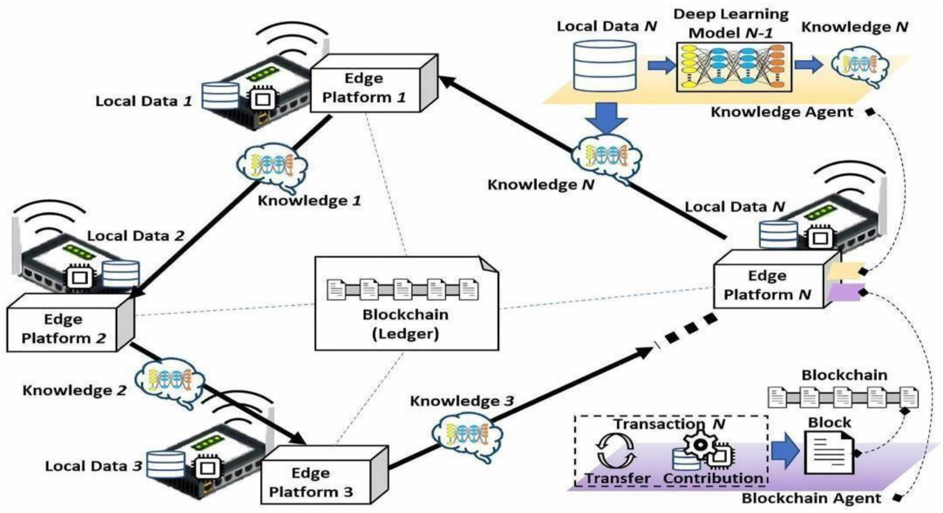
Ramalingam and Mohan's[5] (2021) research examines the role of semantic standards in enabling portability and interoperability in multi-cloud systems. These settings, which use several cloud platforms, suffer obstacles such as vendor lock-in and compatibility issues due to the lack of unifying standards. The study underlines the importance of standardised frameworks, ontology-based techniques, and APIs for enabling seamless data flow and integration across cloud platforms. It also emphasizes the importance of collaboration between cloud providers and industry stakeholders in tackling these issues. The paper proposes methods to improve interoperability and portability, paving the way to overcome constraints in multi-cloud ecosystems.

3. CHALLENGE DEFINITION

3.1 Decentralized Architecture

Edge computing employs a decentralized approach [6] where data processing occurs closer to the source rather than relying on centralized data centers. This setup minimizes latency and boosts performance, making it ideal for applications like IoT, autonomous vehicles, and video streaming. However, the distributed nature of edge networks complicates data management

Fig: 1 Decentralized edge computing architecture [7]



security enforcement across geographically dispersed nodes.

3.2 Vast Attack Surface

The decentralized architecture inherent in edge computing significantly expands the security landscape, revealing additional entry points vulnerable to cyber assaults. Malicious actors can target network components such as endpoint devices, routers, and switches, potentially aiding unlawful penetration and compromising confidential data. The dynamic and distributed nature of edge computing challenges security management since data is generally processed closer to the source rather than in centralized systems, leaving gaps for attackers to exploit. To secure sensitive information, these weaknesses must be addressed by deploying resilient security frameworks and using diligent threat-monitoring methods.

3.3 Heterogeneous Device Ecosystem

Edge computing networks comprise devices with diverse configurations, operating systems, and capabilities. This heterogeneity poses challenges in implementing uniform security standards, as a one-size-fits-all approach is often ineffective. Developing adaptable security frameworks that cater to varying device specifications is essential for maintaining network integrity. 3.3 Complex Authentication and Authorization In contrast to centralized cloud systems, edge computing involves multiple geographically dispersed devices, complicating authentication and authorization processes [8]. Ensuring secure access requires advanced methods such as multi-factor authentication, biometric verification, and granular access controls. These measures not only verify user identities but also prevent unauthorized activities across the network.

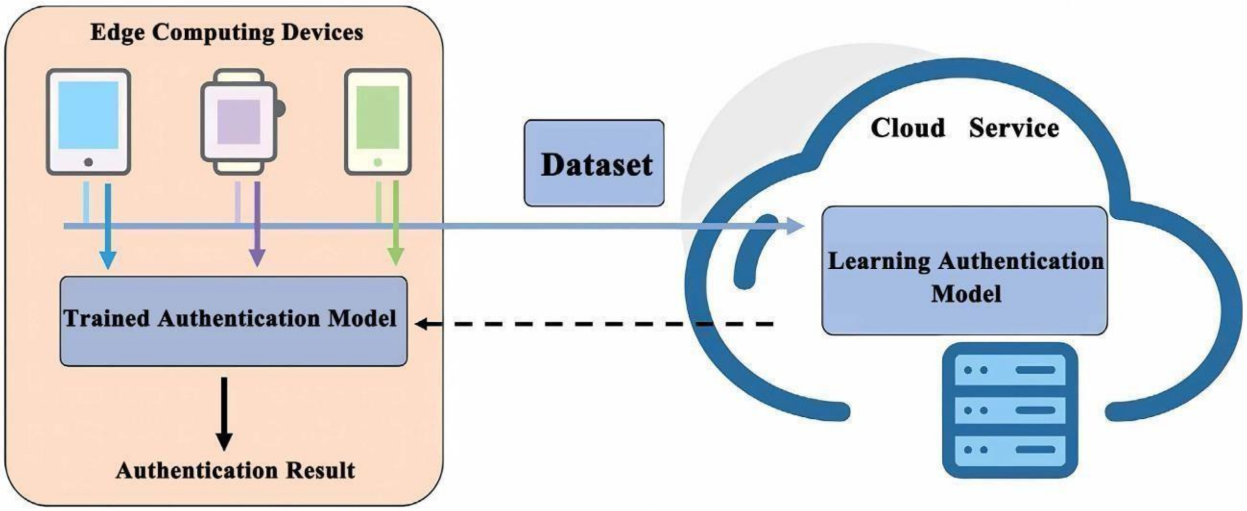
3.4 Complex Authentication and Authorization

In contrast to centralized cloud systems, edge computing involves multiple geographically dispersed devices, complicating authentication and authorization processes [9]. Ensuring secure access requires advanced methods such as multi-factor authentication, biometric verification, and granular access controls. These measures not only verify user identities but also prevent unauthorized activities across the network.

3.5 Data Privacy and Encryption Challenges

Protecting sensitive data as it traverses between edge devices and the cloud [10], is a major concern. Implementing end-to-end encryption ensures data confidentiality, but managing compliance with privacy regulations in decentralized environments remains complex.

Organizations must adopt advanced encryption standards and enforce strict data handling practices to safeguard information integrity.



Fig; 2 Accuracy and authentication in edge computing [11]

3.6 Physical Security of Edge Devices

Edge devices are often deployed in remote or low-security environments, making them open to physical tampering [12]. Securing these devices requires a combination of physical safeguards, regular software updates, and firmware patches. Incorporating secure hardware designs and tamper-resistant features further strengthens their defense against breaches.

4. METHODLOGY

4.1 Research Design

4.1.1 Approach

This study adopts a qualitative research methodology, primarily concentrating on the scrutiny of existing literature. The intention behind this strategy is to delve into various security dimensions associated with edge computing in cloud network.

4.1.2 Reasoning

This approach is thought to be the best for determining the role of edge computing in cloud networks and investigating how security measures might be enhanced. It provides a comprehensive understanding of edge computing’s involvement in cloud infrastructures, empowering researchers to gather intricate, context-specific data that fosters valuable discoveries in this domain. Furthermore, it offers human-centric perspectives by engaging with individuals or organizations, facilitating decision-making and a nuanced understanding of human factors.

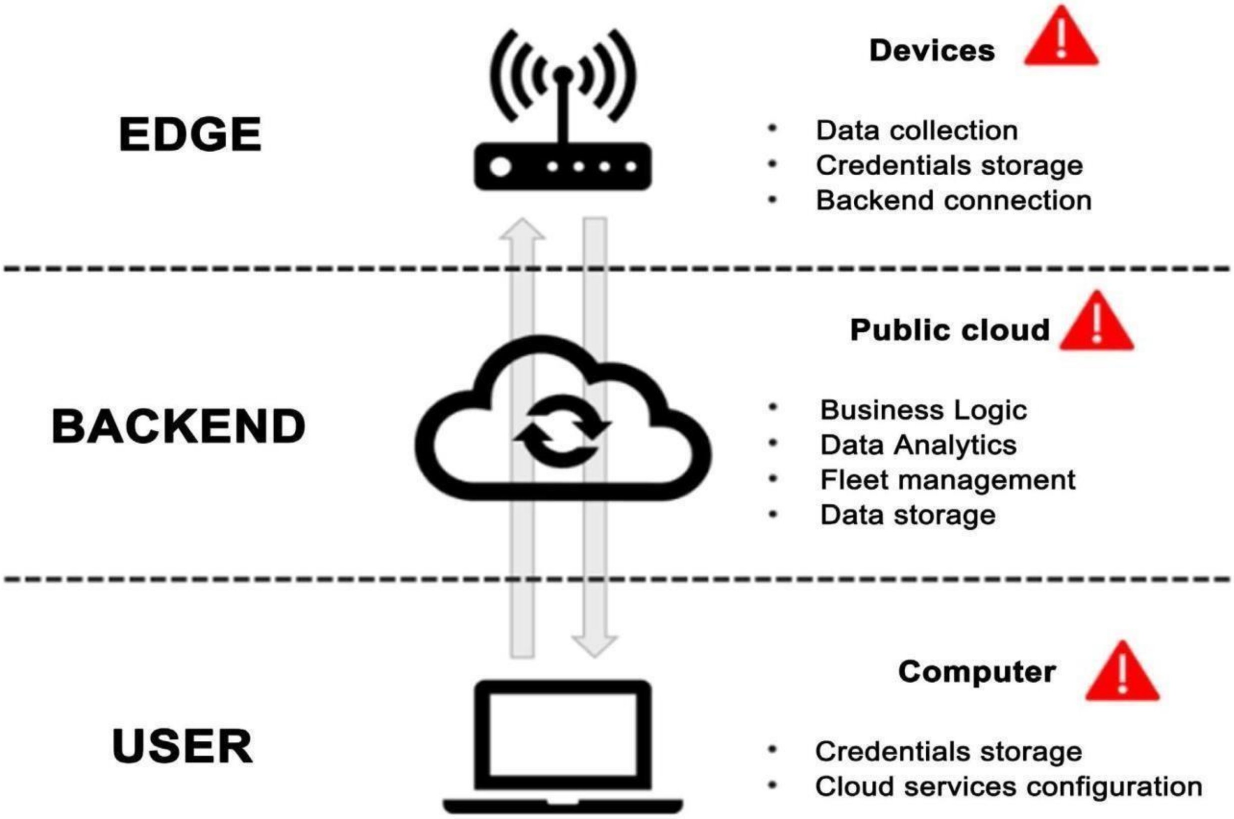


Fig: 3. Confidentiality in edge computing

4.2 Data Collection Method

4.2.1 Selection Criteria

The data collection for this study draws from a diverse range of sources, including books, conference papers, and academic journals published between 2020 and 2023[13]. This temporal scope ensures the information is contemporary, reflecting the current state of security challenges in edge computing within an advanced technological landscape. These inclusion criteria prioritize sources addressing security constraints in edge computing, ensuring alignment with the study's objectives.

4.2.2 Search Process

The research employs a methodical search strategy across prominent databases such as the

ACM Digital Library and IEEE Xplore[14]. Relevant keywords, including terms like cloud network security and edge computing security, are used to ensure the review encompasses literature closely tied to the research's aims.

4.2.3 Selection Process

The selection procedure meticulously filters abstracts, titles, and pertinent texts that directly relate to the research objectives. The focus is on selecting studies that offer significant insights into the security challenges and considerations pertinent to edge computing within cloud networks. This process ensures that only high-quality, relevant information is included, thereby contributing to a well-informed analysis of security implications in this domain.

4.3 Data Analysis Techniques

4.3.1 Synthesis of Findings

Data analysis is a critical component of this study, encompassing the synthesis of key findings extracted from the selected literature. This involves summarizing each study's insights, identifying recurring themes, and categorizing the information pertaining to the security implications of edge computing in cloud environments.

4.3.2 Pattern Analysis

Thematic analysis focuses on evaluating the data by identifying distinct themes and patterns. It serves to uncover overarching trends related to the research's core concerns.

4.3.3 .Gap Recognition

The collected data is rigorously examined to pinpoint gaps in existing studies, highlighting areas that warrant further research. Identifying these gaps provides a foundation for future inquiry into the security dimensions of edge computing within cloud networks, addressing issues such as vulnerabilities and potential threats to cloud systems.

5.SECURITY CHALLENGES

Edge Device Security Risks

Devices deployed in resource-constrained and geographically dispersed zones present critical security gaps. Limited computational capacity, energy resources, and defensive measures render them susceptible to physical tampering[15] and unauthorized access. To mitigate these exposures, comprehensive encryption algorithms, vigilant surveillance systems, and hardware-level protections are indispensable.

Secure Data Communication

Frequent data transmissions between edge nodes and central servers amplify risks of eavesdropping and interception. Heightened concerns around privacy demand rigorous encryption protocols, secure communication channels, and systematic oversight to reinforce data integrity[during transit.

Distributed Authentication and Authorization

Traditional centralized authentication frameworks falter within decentralized architectures. Edge systems necessitate adaptive identity management solutions leveraging advanced cryptographic tools to safeguard access. Distributed authentication paradigms emerge as imperative safeguards, offering robust barriers against intrusions.

Resource Allocation and Isolation

Efficient resource allocation and workload compartmentalization underpin edge security. Improper isolation within shared environments raises susceptibility to breaches and data leaks. Solutions such as virtualization and containerization ensure isolated, secure operational domains, preserving data sovereignty and system integrity.

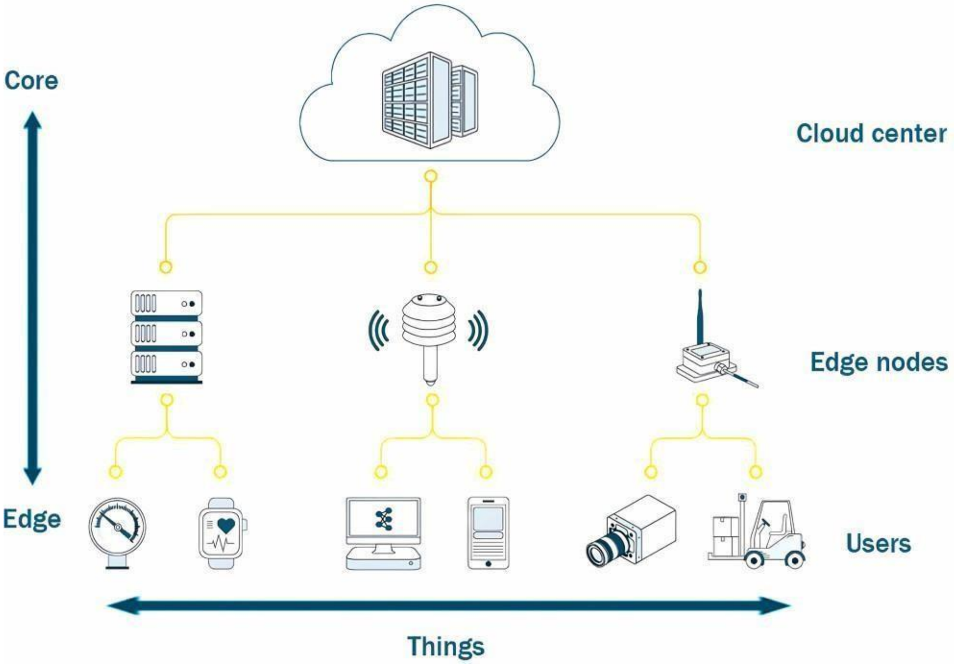


Fig: 4 Resource management in edge computing[16]

Regulatory Obligations

Navigating diverse legal frameworks poses hurdles for edge computing systems, particularly when data traverses jurisdictions. Ensuring alignment with global privacy mandates, including GDPR, requires meticulous governance protocols and auditable workflows to harmonize compliance with distributed infrastructures[17].

6.SECURITY SOLUTIONS

Edge Device Protection Standards

Fortifying edge devices[18] necessitates rigorous protocols encompassing firmware updates, secure boot processes, and tamper-resistant enclosures. Regular updates address evolving threats, ensuring resilience. Secure boot mechanisms validate software authenticity, safeguarding against malicious code infiltration.

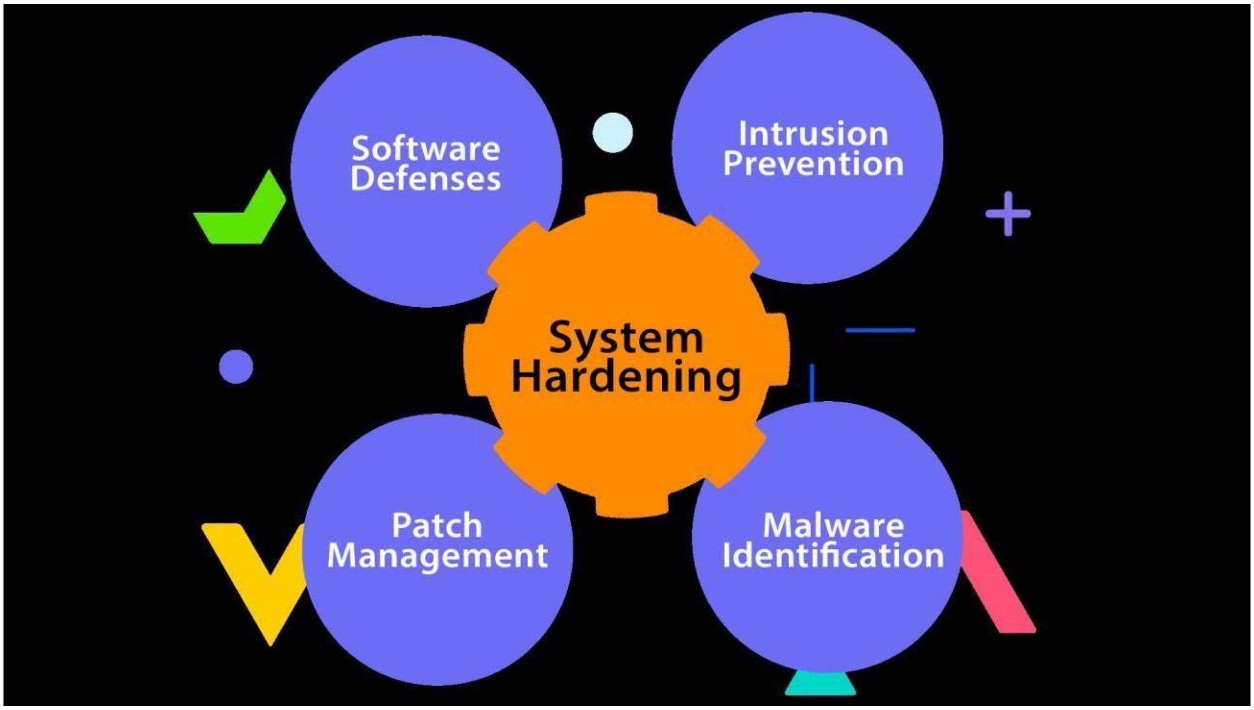


Fig 5: Edge device hardening[19]

Secure Communication Protocols

End-to-end encryption, complemented by Transport Layer Security (TLS), establishes impregnable communication channels, shielding sensitive data from interception and manipulation. Such measures preserve confidentiality and integrity, reinforcing trust across distributed nodes.

Distributed Identity Management

Block-chain-based identity frameworks introduce tamper-proof authentication layers, decentralizing security controls to counter vulnerabilities inherent in traditional systems. These innovations align with the distributed nature of edge computing, ensuring reliability and scalability becomes fundamental for robust authentication, particularly in edge-based ecosystems. Such methodologies bolster the structural defenses of these architectures, ensuring seamless yet fortified interactions.

7.RESULTS AND DISCUSSION

The integration of edge computing into cloud network frameworks heralds a transformative era in distributed data processing, offering enhanced computational efficiency, reduced latency, and a seamless user experience. However, these advancements come with multifaceted security challenges that necessitate robust countermeasures. Edge devices, often deployed in resource-constrained and geographically dispersed environments, face vulnerabilities such as physical tampering, unauthorized access, and malware attacks. Secure data communication is another critical concern, as frequent exchanges between edge nodes and central servers amplify risks of eavesdropping and data manipulation. To address these issues, advanced encryption protocols, secure communication channels like Transport Layer Security (TLS), and tamper-resistant hardware are vital. Additionally, traditional centralized authentication frameworks fall short in decentralized edge architectures, underscoring the need for adaptive solutions like blockchain-based identity management frameworks that provide scalable and tamper-proof authentication. Effective resource allocation through virtualization and containerization ensures isolated operational domains, safeguarding data integrity and sovereignty. Regulatory compliance adds another layer of complexity, especially when data traverses jurisdictions, requiring meticulous governance and adherence to privacy mandates such as GDPR.

This study highlights the importance of fortifying edge devices with secure boot processes and regular firmware updates, enhancing communication protocols, and leveraging distributed identity management solutions. Identifying gaps in existing literature—such as universal standards for edge security and adaptive compliance mechanisms—provides avenues for future research.

Overall, the adoption of dynamic, evolving security architectures is essential for mitigating risks and bolstering the resilience of edge computing ecosystems.

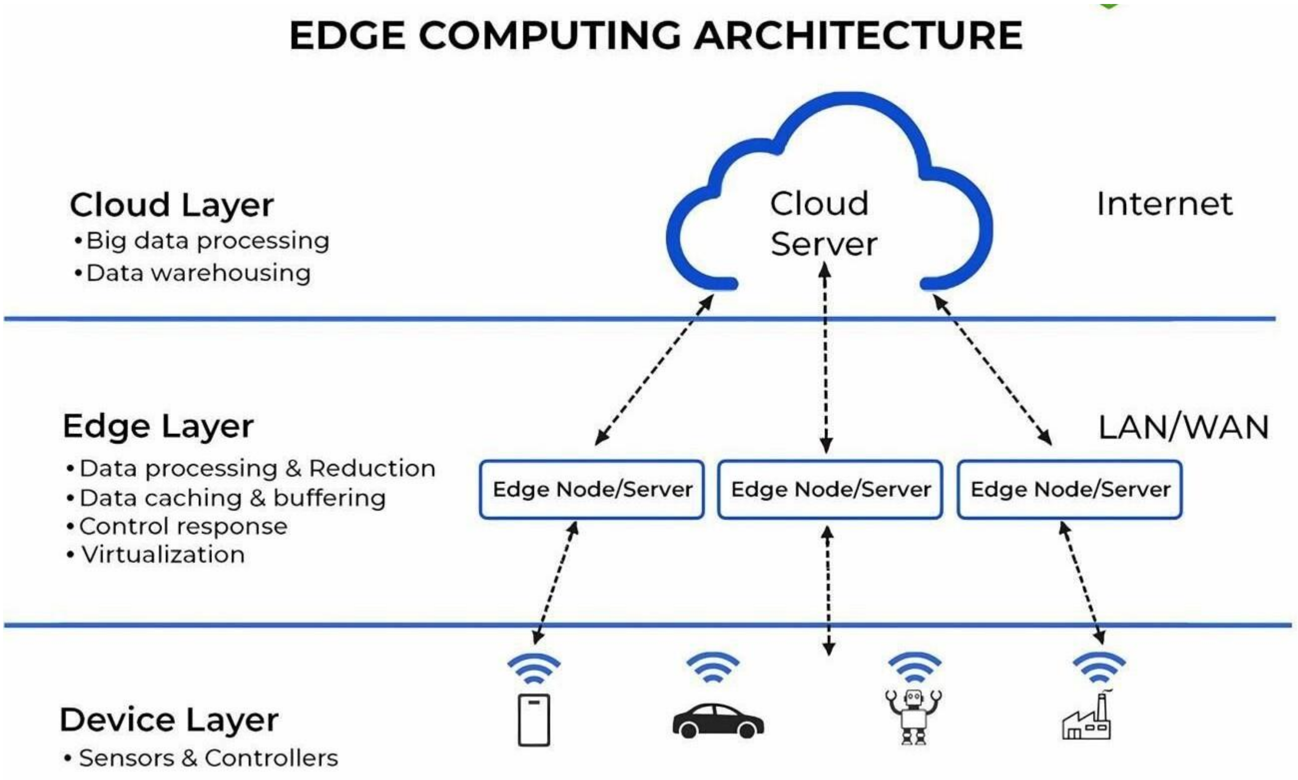


Fig: 6 Edge computing in cloud network architecture [20]

8.CONCLUSION

In conclusion, the security paradigms underlying edge computing frameworks within cloud infrastructures are a complex tapestry of benefits, limitations, and daunting problems that organizations must overcome. The intrinsically decentralized topology of edge computing improves data handling efficiency, resulting in a paradigm shift in processing approaches. However, decentralization creates an urgent need for reinforced and adaptive security techniques, emphasizing the importance of blockchain integration as a cornerstone for strengthening defenses within these distributed ecosystems. Prioritizing the inviolability and confidentiality of data, whether in rest or traveling convoluted digital conduits, is critical. Such imperatives are motivated by the dual imperatives of reducing vulnerabilities related to data secrecy while also alleviating constraints imposed by restricted processing resources.

9.REFERENCES

[1] Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020) A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. *The Journal of Supercomputing*, **76**,9493-9532.
[2] Abdulsalam, Y.S. and Hedabou, M. (2021) Security and Privacy in Cloud Computing: Technical Review. *Future Internet*, **14**, 11-15.

[3] Cao, K., Liu, Y., Meng, G. and Sun, Q. (2020) An Overview on Edge Computing Research. *IEEE Access*, **8**, 85714-85728.

[4] Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B. and Hakak, S. (2022)Cloud Computing Security: A Survey of Service-Based Models. Computers & Security, 114, Article ID: 102580.

[5] Ramalingam, C. and Mohan, P. (2021) Addressing Semantics Standards for CloudPortability and Interoperability in a Multi-Cloud Environment. Symmetry , 13, Article317.

[6] Atieh, A.T. (2021) The Next Generation Cloud Technologies: A Review on Distributed Cloud, Fog and Edge Computing and Their Opportunities and Challenges ResearchBerg Review of Science and Technology , 1, 1-15.

[7] Jin, W., Xu, Y., Dai, Y. and Xu, Y. (2023) Blockchain-Based Continuous KnowledgeTransfer in Decentralized Edge Computing Architecture. Electronics, 12, Article 1154.

[8] Ning, H., Li, Y., Shi, F. and Yang, L.T. (2020) Heterogeneous Edge Computing OpenPlatforms and Tools for the Internet of Things. Future Generation Computer Systems,
106, 67-76.

[9] . O., Oyeniran, O. C., Adewusi, A. O., Komolafe, A. M., & Obijuru, A. (2024). Reviewing the transformational impact of edge computing on real-time data processing and analytics. *CSIT Research Journal*, *5*(3). https://doi.org/10.51594/csitrj.v5i3.929
[10] Alwarafy, A., Al-Thelaya, K.A., Abdallah, M., Schneider, J. and Hamdi, M. (2020) ASurvey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things.IEEE Internet of Things Journal , 8, 4004-4022.

[11] Zeng, X., Zhang, X., Yang, S., Shi, Z. and Chi, C. (2021) Gait-Based Implicit Authentication Using Edge Computing and Deep Learning for Mobile Devices. Sensors , 21,

Article 4592. https://www.mdpi.com/1424-8220/21/13/4592

[12] Sha, K., Yang, T.A., Wei, W. and Davari, S. (2020) A Survey of Edge Computing-BasedDesigns for IoT Security. Digital Communications and Networks , 6, 195-202.

[13] Raja, V., & Chopra, B. (2024). Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns. *Journal of Advanced Information and Global Studies*, *4*(1).

[14] Mishra, S.B. and Alok, S. (2022) Handbook of Research Methodology. Educreation publishing, Delhi.

[15] Mourão, E., Pimentel, J.F., Murta, L., Kalinowski, M., Mendes, E. and Wohlin, C.(2020) Onthe Performance of Hybrid Search Strategies for Systematic LiteratureReviews in Software Engineering. Information and Software Technology, 123, Article ID: 106294.

[16] Wani, R. U. Z., Thabit, F., & Can, O. (2024). Security and privacy challenges, issues, and enhancing techniques for the Internet of Medical Things: A systematic review. *Security and Privacy*, *7*(1), Article e409.

[17] He, Z., Zhang, T. and Lee, R.B. (2020) Attacking and Protecting Data Privacy inEdge-Cloud Collaborative Inference Systems. IEEE Internet of Things Journal , 8,9706-9716.

[18] Liu, H., Li, S. and Sun, W. (2020) Resource Allocation for Edge Computing withoutUsing Cloud Center in Smart Home Environment: A Pricing Approach. Sensors, 20,Article 6545.

[19] Benjamin, A. (2022) What Is System Hardening? Standards and Best Practices.

[20] Mohanan, R. (2022) What Is Edge Computing? Components, Examples, and Best Practices.