INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

COMPREHENSIVE EXPLORATION OF CLOUD AND EDGE COMPUTING SECURITY: DEFENSE MECHANISMS, ADAPTIVE ALGORITHMS, AND THREAT DETECTION STRATEGIES

M. Gayathri[1], Dr. G. Srinaganya[2]

[1]Research scholar, Department of computer science, National College(Autonomous), Trichy, Tamilnadu, India
[2]Assistant Professor, Department of computer science, National College(Autonomous), Trichy, Tamilnadu, India

ABSTRACT

The exploration encompasses key concepts including cloud computing, edge computing, defense mechanisms, adaptive algorithms, attack detection, and overall security considerations.This survey provides a comprehensive examination of recent academic journals, offering insights into the dynamic landscape of cloud and edge computing security. Beginning with an overview of the current state of cloud computing, the survey highlights advancements in architecture, service models, and deployment strategies. It then transitions into the evolving realm of edge computing, emphasizing its decentralized nature and the resulting implications for security in distributed environments.A significant portion of the survey is dedicated to elucidating the latest developments in cloud defense mechanisms. Researchers are actively addressing vulnerabilities in cloud infrastructures, proposing innovative solutions such as encryption techniques, access controls, and anomaly detection. The synthesis of findings from multiple journals provides a comprehensive understanding of these defense mechanisms and their effectiveness in countering diverse cyber threats.Adaptive algorithms emerge as a crucial component in this survey, demonstrating their role in dynamically adjusting systems to evolving threats. The exploration extends to the latest adaptive algorithms designed to bolster the resilience of cloud and edge systems, enabling real-time responses to emerging threats. Moreover, the survey delves into attack detection mechanisms, examining challenges associated with identifying and mitigating cyber threats in cloud and edge environments. Signature-based, anomaly-based, and behavior-based detection techniques are discussed within the context of securing these infrastructures.

KEYWORDS: Cloud Computing, Edge Computing, Defence Mechanisms, Adaptive Algorithms, Attack Detection, Security Considerations

I. INTRODUCTION

In response to the widespread use of mobile devices and the growing demand for applications with low latency and high throughput, Mobile Edge Computing (MEC) has emerged as a promising paradigm for offloading computational tasks to the network edge. However, the dynamic and resource-constrained nature of

MEC environments brings forth new challenges, particularly in terms of security. Addressing these challenges becomes imperative to ensure the integrity and confidentiality of sensitive data processed at the edge. This paper introduces a pioneering Secured Edge Computing Intrusion Detection System (SEC-IDS) specifically designed for MEC environments [1]. The proposed SEC-IDS framework seamlessly integrates both signature-based and anomaly-based detection mechanisms, aiming to elevate the precision and adaptability of intrusion detection. By capitalizing on edge computing resources, the framework strategically distributes detection tasks closer to the data source, thereby reducing latency and enhancing real-time responsiveness. The effectiveness of the SEC-IDS framework is rigorously assessed through extensive experiments conducted in a simulated MEC environment.

The intersection of security and energy efficiency in Wireless Sensor Networks (WSNs) employs blockchain technology. The study focuses on the imperative need to enhance the security infrastructure of WSNs while concurrently addressing energy efficiency concerns. The authors propose a novel approach that integrates blockchain mechanisms into the WSN framework, aiming to fortify the network's security protocols [2]. By leveraging the decentralized and tamper-resistant nature of blockchain, the study seeks to establish a robust defence against potential security threats. Furthermore, the paper explores the potential impact of this blockchain-integrated security strategy on the overall energy efficiency of WSNs. This literature survey encapsulates the key contributions and insights presented in the journal article, shedding light on the innovative amalgamation of blockchain technology with WSNs for ensuring both security and energy efficiency.

II. CLOUD INFUSED PRECISION REVOLUTIONIZED TESTING STRATEGIES FOR ROBUST IOT APPLICATIONS

Bukhsh et al. (2023) explores an innovative application of Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) in approximating the roots, or eigenvalues, of the transcendental equation associated with the cantilever beam [3]. The study delves into the realm of structural engineering and computational mathematics, introducing a novel computational approach to address a fundamental problem in structural analysis. The utilization of LSTM-RNN in approximating eigenvalues adds a layer of sophistication to the traditional methods applied in structural engineering. The authors aim to enhance the accuracy and efficiency of eigenvalue computation for cantilever beams, a critical aspect in understanding and optimizing the structural behaviour. The literature survey encapsulates the unique contributions of the journal article, highlighting the integration of advanced machine learning techniques into the domain of structural analysis, with a specific focus on the application of LSTM-RNN for approximating roots in the transcendental equation of cantilever beams. This innovative approach has the potential to significantly impact the field by offering a more accurate and computationally efficient solution to a longstanding problem in structural engineering.

Naqvi et al. (2022) delves into the domain of Internet of Things (IoT) applications, presenting a comprehensive exploration of ontology-driven testing strategies [4]. In the rapidly evolving landscape of IoT, ensuring the reliability and functionality of applications is paramount. The authors propose an innovative approach that leverages ontology-driven testing to address the intricacies of IoT applications. The integration of ontologies, which formalize domain knowledge, into testing strategies offers a systematic and knowledge-driven framework for evaluating IoT applications. The study investigates various testing methodologies and strategies, emphasizing the role of ontologies in enhancing test case generation, coverage, and overall testing effectiveness. By aligning testing processes with ontological structures, the authors aim to improve the adaptability and efficiency of testing procedures in the context of IoT applications. The literature survey encapsulates the key findings and insights of the journal article, shedding light on the significance of ontology-driven testing strategies in the realm of IoT, with a focus on their potential to enhance the reliability and robustness of IoT applications through a knowledge-centric testing paradigm.

The journal authored by Ashraf et al. (2020) presents a survey on the innovative application of Internet of Things (IoT) edge technologies for the detection and tracking of contagion during the COVID-19 pandemic

[5]. In response to the global health crisis, the study explores the integration of IoT-edge technologies as a means to efficiently monitor and manage contagion spread. The authors delve into the technical aspects and methodologies employed in detecting and tracking contagion, presenting insights derived from the 2020 International Conference on Electrical, Communication, and Computer Engineering. The survey underscores the role of IoT-edge technologies in providing real-time data, enabling timely responses to mitigate the impact of the pandemic. The findings contribute to the ongoing discourse on leveraging technological solutions for public health emergencies, offering valuable insights into the practical implementation of IoT-edge technologies for contagion monitoring and control.Mumtaz et al. (2023) present a notable contribution to the field of cybersecurity focusing on the proactive identification of cyber threats, the authors leverage advanced data mining and machine learning techniques to classify and predict significant cyber incidents [6]. The study holds potential implications for enhancing cyber defense strategies by providing a predictive framework for cybersecurity professionals.

Ahmed et al. (2022) introduce "AAQAL," a Machine Learning-Based Tool for Performance Optimization of Parallel SPMV Computations Using Block CSR addresses the critical area of parallel computations, specifically Single Program Multiple Data (SPMV) computations [7]. The authors employ machine learning techniques to develop AAQAL, aiming to optimize the performance of parallel SPMV computations through Block Compressed Sparse Row (CSR). This tool offers potential advancements in the efficiency of parallel computing applications. Almogren (2020) delves into the realm of Edge-of-Things (EoT) computing with a focus on Intrusion detection in Edge-of-Things computing investigates the intricacies of intrusion detection within EoT computing environments, addressing the unique challenges posed by the distributed and resource-constrained nature of edge computing [8]. The findings contribute to the ongoing discourse on securing Edge-of-Things systems.

Li et al. (2020) contributes to the field of intrusion detection in edge computing networks with their work on GLIDE: A Game Theory and Data-Driven Mimicking Linkage Intrusion Detection for Edge Computing Networks published in Complexity [9]. The authors propose a novel intrusion detection system, GLIDE, which combines game theory principles with data-driven mimicking linkage to enhance the security of edge computing networks. This research provides valuable insights into the development of advanced intrusion detection mechanisms tailored for the unique characteristics of edge computing networks.

III. CUTTING-EDGE INSIGHTS: EXPLORING RECENT ADVANCES IN CLOUD COMPUTING THROUGH COMPREHENSIVE SURVEYS

Rivera et al. (2021) contribute to the infrastructure security with their work on Robust Authentication and Data Flow Integrity for P2P SCADA Infrastructures addresses the critical challenges in securing Peer-to-Peer (P2P) SCADA systems [10]. The authors focus on robust authentication mechanisms and data flow integrity to enhance the security posture of SCADA infrastructures, shedding light on the unique vulnerabilities in these systems. .Alsubhi et al. (2020) present "MEACC," an energy-efficient framework for smart devices utilizing cloud computing systems propose MEACC as an innovative solution to optimize energy consumption in smart devices by leveraging cloud computing [11]. This research contributes to the development of sustainable and efficient frameworks for the integration of smart devices within cloud computing ecosystems.Long et al. (2024) introduce a Transformer-based network intrusion detection approach for cloud security explores the application of Transformer-based models for enhancing network intrusion detection in cloud environments [12]. This research represents a significant advancement in leveraging state-of-the-art deep learning techniques for cloud security.

Liu et al. (2023) investigate Joint task offloading and resource allocation for device-edge-cloud collaboration with subtask dependencies present a comprehensive approach to optimize task offloading and resource allocation in collaborative device-edge-cloud environments, addressing subtask dependencies. This research contributes to the ongoing efforts in enhancing the efficiency of device-edge-cloud collaborations [13].Cheng et al. (2023) propose a deep reinforcement learning-based preemptive approach for cost-aware cloud

job scheduling focuses on optimizing cloud job scheduling by incorporating deep reinforcement learning to preemptively address cost-aware considerations [14]. The research aims to enhance the economic efficiency of cloud job scheduling strategies.Zhang et al. (2023) tackle the challenge of File processing security detection in multi-cloud environments using a process mining approach, as published in the Journal of Cloud Computing. The authors provide insights into securing file processing in multi-cloud environments through innovative security detection methodologies, emphasizing the use of process mining techniques [15].

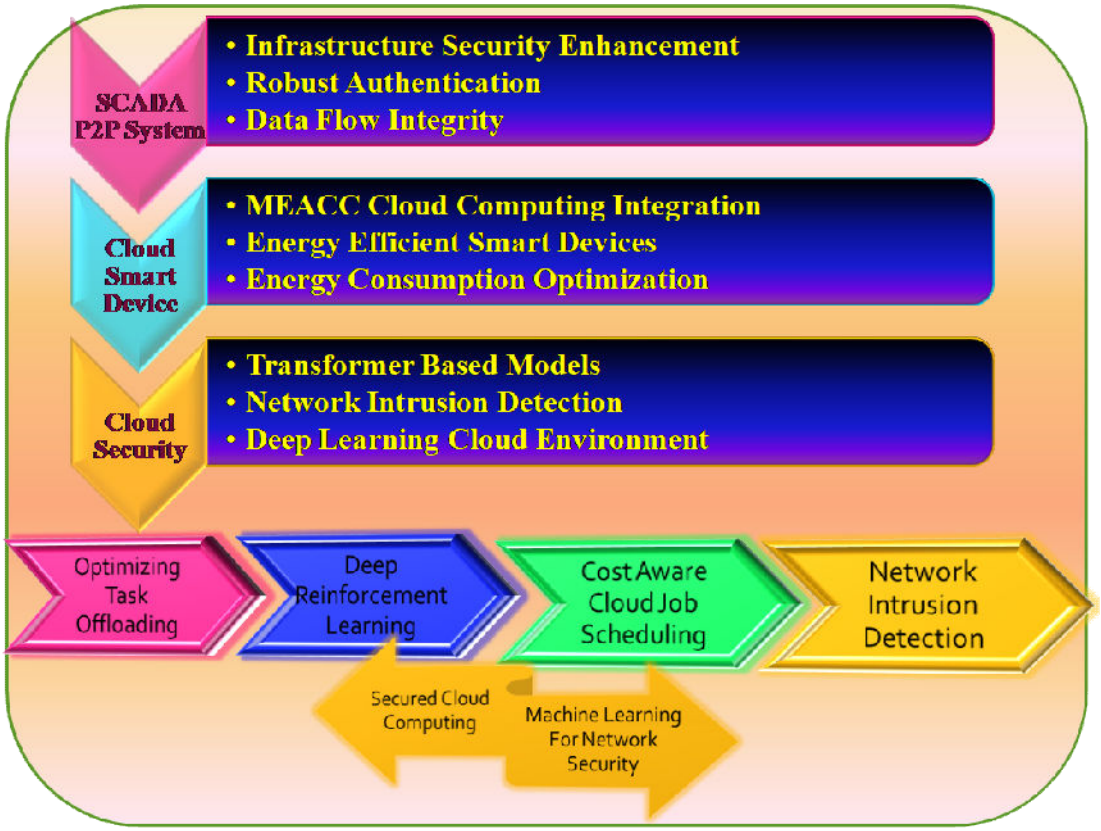

Figure 1 Diagram Depicting Various Cloud Edge Computing Models

Jangjou and Sohrabi (2022) present A comprehensive survey on security challenges in different network layers in cloud computing in the Archives of Computational Methods in Engineering. The survey offers a holistic examination of security challenges across various network layers in cloud computing, providing a valuable resource for understanding and mitigating security risks in cloud environments [16].Wu et al. (2021) contribute to the domain of network intrusion detection with their research on Research on network intrusion detection technology based on machine learning focuses on advancing intrusion detection technology through machine learning, providing insights into the application of machine learning techniques for enhancing network security [17].

IV. PERFORMANCE DISCUSSIONS AND ANALYSIS

The discussion offers a diverse array of insights into recent advances in computing. The first study focuses on robust authentication and data flow integrity in peer-to-peer SCADA infrastructures. The authors delve into authentication robustness and data flow integrity, presenting advancements in securing SCADA networks. Shifting focus to energy efficiency and cloud computing, the second study introduces a framework for enhancing energy efficiency in smart devices through cloud computing systems. This work provides valuable insights for sustainable and resource-conscious computing.Moving on to network security, the third study proposes a transformer-based network intrusion detection approach for cloud security. The novel intrusion

detection strategy based on transformer networks suggests potential advancements in cloud security through sophisticated machine learning techniques. In the realm of resource allocation and scheduling, the fourth study investigates joint task offloading and resource allocation for device-edge-cloud collaboration. This work sheds light on optimizing collaboration between devices, edge, and cloud resources, contributing to more efficient and dynamic cloud computing ecosystems.

Focusing on job scheduling, the fifth study presents a deep reinforcement learning-based pre-emptive approach for cost-aware cloud job scheduling. This innovative approach offers a dynamic and adaptive solution, addressing challenges related to cost optimization in cloud environments. The sixth study delves into file processing security detection in multi-cloud environments through a process mining approach. This work provides insights into enhancing security in multi-cloud environments, emphasizing the importance of efficient file processing security detection.In a broader context, the seventh study offers a comprehensive survey on security challenges in different network layers in cloud computing. This survey serves as a foundational resource for understanding and addressing security concerns across various network layers in cloud environments. Lastly, the eighth study contributes to the field of network security by focusing on machine learning-based intrusion detection technology. This research adds to the ongoing discourse on bolstering network security through advanced computational approaches. In conclusion, these consolidated insights collectively showcase the cutting-edge developments in computing, spanning security enhancements, energy efficiency, machine learning applications, and novel approaches to scheduling and resource allocation in cloud environments.

V. CONCLUSION

In conclusion, the survey consolidates insights on overarching security considerations in cloud and edge computing, emphasizing the need for a holistic approach that includes aspects of data privacy, compliance, and regulatory adherence. This synthesis contributes valuable knowledge to the ongoing discourse, catering to researchers, practitioners, and policymakers engaged in securing these critical computing environments.This survey underscores the dynamic evolution and multifaceted challenges inherent in securing cloud and edge computing environments. The synthesis of recent academic journals provides a panoramic view of advancements in cloud architecture, innovative defense mechanisms, adaptive algorithms, and sophisticated attack detection strategies. The findings emphasize the imperative for a holistic security approach, addressing not only the technical aspects but also encompassing data privacy, compliance, and regulatory considerations. As cloud and edge technologies continue to reshape the digital landscape, the insights gleaned from this survey contribute to a deeper understanding of the intricacies involved in safeguarding these distributed systems. This knowledge serves as a valuable resource for researchers, practitioners, and policymakers seeking to fortify the resilience of cloud and edge computing infrastructures against an ever-evolving spectrum of cyber threats.

VI. REFERENCES

1. Alsubhi, K. A Secured Intrusion Detection System for Mobile Edge Computing. *Appl. Sci.* **2024**, *14*, 1432. https://doi.org/10.3390/app14041432
2. Rehman, A.; Abdullah, S.; Fatima, M.; Iqbal, M.W.; Almarhabi, K.A.; Ashraf, M.U.; Ali, S. Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain. *Appl. Sci.* **2022**, *12*, 10794.
3. Bukhsh, M.; Ali, M.S.; Alourani, A.; Shinan, K.; Ashraf, M.U.; Jabbar, A.; Chen, W. Long Short-Term Memory Recurrent Neural Network Approach for Approximating Roots (Eigen Values) of Transcendental Equation of Cantilever Beam. *Appl. Sci.* **2023**, *13*, 2887.
4. Naqvi, M.R.; Iqbal, M.W.; Ashraf, M.U.; Ahmad, S.; Soliman, A.T.; Khurram, S.; Shafiq, M.; Choi, J.-G. Ontology Driven Testing Strategies for IoT Applications. *Comput. Mater. Contin.* **2022**, *70*, 5855–5869.
5. Ashraf, M.U.; Hannan, A.; Cheema, S.M.; Ali, Z.; Alofi, A. Detection and tracking contagion using IoT-edge technologies: Confronting COVID-19 pandemic. In Proceedings of the 2020 International

Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; pp. 1–6

6. Mumtaz, G.; Akram, S.; Iqbal, W.; Ashraf, M.U.; Almarhabi, K.A.; Alghamdi, A.M.; Bahaddad, A.A. Classification and Prediction of Significant Cyber Incidents (SCI) using Data Mining and Machine Learning (DM-ML). *IEEE Access* **2023**, *11*.
7. Ahmed, M.; Usman, S.; Shah, N.A.; Ashraf, M.U.; Alghamdi, A.M.; Bahadded, A.A.; Almarhabi, K.A. AAQAL: A Machine Learning-Based Tool for Performance Optimization of Parallel SPMV Computations Using Block CSR. *Appl. Sci.* **2022**, *12*, 7073.
8. Almogren, A.S. Intrusion detection in Edge-of-Things computing. *J. Parallel Distrib. Comput.* **2020**, *137*, 259–265.
9. Li, Q.; Hou, J.; Meng, S.; Long, H. GLIDE: A Game Theory and Data-Driven Mimicking Linkage Intrusion Detection for Edge Computing Networks. *Complexity* **2020**, *2020*, 7136160.
10. Rivera, A.O.G.; White, E.M.; Tosh, D.K. Robust Authentication and Data Flow Integrity for P2P SCADA Infrastructures. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 7 September 2021; pp. 557–564.
11. Alsubhi, K.; Imtiaz, Z.; Raana, A.; Ashraf, M.U.; Hayat, B. MEACC: An energy-efficient framework for smart devices using cloud computing systems. *Front. Inf. Technol. Electron. Eng.* **2020**, *21*, 917–930.
12. Long, Z., Yan, H., Shen, G. *et al.* A Transformer-based network intrusion detection approach for cloud security. *J Cloud Comp* **13**, 5 (2024). https://doi.org/10.1186/s13677-023-00574-9
13. Liu F, Huang J, Wang X (2023) Joint task offloading and resource allocation for device-edge-cloud collaboration with subtask dependencies. IEEE Trans Cloud Comput 11(3):3027–3039
14. Cheng L, Wang Y, Cheng F, Liu C, Zhao Z, Wang Y (2023) A deep reinforcement learning-based preemptive approach for cost-aware cloud job scheduling. IEEE Trans Sustain Comput
15. Zhang X, Cui L, Shen W, Zeng J, Du L, He H, Cheng L (2023) File processing security detection in multi-cloud environments: a process mining approach. J Cloud Comput 12(1):100
16. Jangjou M, Sohrabi MK (2022) A comprehensive survey on security challenges in different network layers in cloud computing. Arch Comput Methods Eng 29(6):3587–3608
17. Wu, Fei, Ting Li, Zhen Wu, ShuLin Wu, and ChuanQi Xiao (2021) Research on network intrusion detection technology based on machine learning. Int J Wireless Inf Netw 28(no. 3):262–275