Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 5
May 2025

Securing the Edge: A Review of Security as a Service in MEC Environments

Pratik Daund [1], Prof. Dr. M. A. Shah [2]

[1]Walchand College of Engineering, Department of Computer Science, Vishrambag, Sangli, Maharashtra, India.
Email: pratik.daund@walchandsangli.ac.in

[2] Walchand College of Engineering, Department of Computer Science, Vishrambag, Sangli, Maharashtra, India.
Email: medha.shah@walchandsangli.ac.in

Abstract

The integration of Security as a Service (SecaaS) with Multi-Access Edge Computing (MEC) infrastructure represents a transformative advancement in securing distributed systems, particularly in IoT and edge environments. This research focuses on leveraging MEC's low-latency and decentralized architecture to develop scalable and resilient security solutions. The necessity for this research arises from the growing proliferation of IoT devices and real-time applications, which are increasingly vulnerable to sophisticated cyber threats. MEC's proximity-based computation offers unique advantages for implementing robust security measures tailored to resource-constrained environments. This study reviews methodologies such as adaptive resource orchestration, knowledge distillation, transfer learning, and machine learning-enhanced intrusion detection systems (NIDS). Additionally, advanced techniques like Attribute-Based Encryption (ABE) and layered security architectures are examined for their effectiveness in addressing latency-sensitive and privacy-related challenges in MEC contexts. Comparative analyses demonstrate improvements in anomaly detection, scalability, and real-time responsiveness achieved through these approaches. The findings underscore MEC's potential to enhance security scalability and responsiveness while mitigating evolving threats. However, gaps remain in integrating these methodologies into a unified SecaaS-MEC framework. Future directions emphasize incorporating AI-driven analytics and advanced cryptographic techniques to optimize SecaaS for diverse edge computing applications.

Keywords: Multi-Access Edge Computing, Anomaly Detection, Intrusion Detection Systems, Edge Computing Security, SecaaS, Authentication, Security as a Service.

1. Introduction

Security as a Service (SecaaS) platforms with Multi-Access Edge Computing (MEC) infrastructure represents a paradigm shift in addressing the complex cybersecurity challenges faced by distributed and resource-constrained networks. MEC, renowned for its low-latency, proximity-aware, and distributed computation capabilities, has fundamentally transformed network architectures by enabling data processing and computational tasks at the edge, closer to the end-users. This innovative approach is particularly advantageous for the Internet of Things (IoT) and real-time applications, which require secure, scalable, and efficient operations to meet their high-performance demands.

The convergence of SecaaS with MEC introduces a powerful framework designed to mitigate inherent security vulnerabilities within edge-cloud environments. As MEC adoption continues to grow across critical applications ranging from industrial automation to healthcare and smart cities it becomes increasingly vital to develop advanced security mechanisms capable of addressing dynamic, evolving, and multifaceted cyber threats. An integrated SecaaS-MEC framework holds the potential to enhance system performance by optimizing latency, ensuring scalability, and enabling real-time threat detection, thus securing the integrity, confidentiality, and availability of edge ecosystems.

Recent research underscores the necessity of adopting sophisticated methodologies to effectively leverage MEC's decentralized architecture for improved security measures and operational efficiencies. Key techniques explored include adaptive resource orchestration for dynamic threat response, machine learning-based anomaly detection to identify and mitigate sophisticated attacks, and advanced cryptographic protocols for secure data transmission and access control. Additionally, multi-layered security frameworks that combine distributed and centralized

security controls provide robust defenses against a wide range of cyber threats, ensuring system resilience even under adverse conditions.

By synthesizing the strengths of these methodologies, this study aims to pave the way for a unified and scalable SecaaS-MEC framework capable of addressing contemporary and emerging cybersecurity challenges. Such a framework not only ensures robust protection against malicious actors but also empowers edge computing environments with the necessary tools to maintain operational efficiency, adaptability, and scalability in the face of evolving technological demands. This research sets the foundation for future advancements in creating comprehensive, AI-driven, and highly responsive SecaaS platforms tailored specifically for MEC-integrated networks.

2. Related Work

Adaptive Risk-Aware Resource Orchestration for 5G Microservices introduces a framework that employs probabilistic risk assessment to optimize resource allocation within multi-tier edge-cloud systems. This approach is particularly relevant for MEC environments, where dynamic resource demands and security threats coexist. By addressing malicious applications and reducing resource inefficiencies, the framework significantly enhances system resilience, performance, and latency management. However, its scope is primarily limited to resource orchestration, leaving broader security considerations, such as authentication protocols and intrusion detection mechanisms, unexplored. This limitation suggests that while the framework effectively enhances operational efficiency, it does not provide a holistic solution to the complex security challenges prevalent in MEC ecosystems [1].The study on Attribute-Based Management for Secure Kubernetes Cloud Bursting by Femminella et al. introduces a novel framework that integrates Attribute-Based Encryption (ABE) into Kubernetes environments to enhance security and scalability. This approach enables fine-grained access control and dynamic resource allocation, ensuring compliance with privacy regulations while maintaining efficiency in distributed systems. The framework is particularly effective for secure orchestration in MEC contexts, addressing the challenges of resource management and privacy. However, its focus is primarily on access control mechanisms, with limited consideration of broader security requirements such as real-time threat detection, anomaly mitigation, and intrusion prevention, which are essential for a comprehensive security solution [2].

The study on Efficient Authentication in Cloud-Fog-Device Frameworks presents a secure protocol designed to address authentication vulnerabilities in cloud-fog-device ecosystems. By leveraging elliptic curve cryptography and cryptographic hashing, the framework enhances security resilience against key-revelation attacks while minimizing computational overhead, making it highly suitable for resource-constrained environments. The approach effectively ensures robust entity authentication and strengthens the overall security posture of fog networks. However, its scope is limited to authentication processes, with little focus on broader security measures such as real-time threat detection, anomaly management, or advanced encryption techniques, which are crucial for addressing the comprehensive security challenges present in MEC environments[3].The study on Efficient Anomaly Detection for Edge Clouds explores the use of knowledge distillation and transfer learning to develop lightweight models tailored for anomaly detection in resource-constrained edge environments. By transferring learned capabilities from larger models to smaller, efficient ones, this approach achieves high detection accuracy while significantly reducing computational demands. These techniques are particularly effective in addressing the limitations of MEC infrastructures, where resources are often restricted. Despite its strengths in improving scalability and detection efficiency, the study focuses primarily on anomaly detection and does not address other critical security aspects, such as encryption, authentication, or comprehensive threat mitigation, which are essential for a robust MEC security framework[4].

The study on Intrusion Detection in IoT Systems investigates the application of machine learning (ML) algorithms in Network Intrusion Detection Systems (NIDS) tailored for IoT environments within MEC contexts. By leveraging MEC's low-latency and proximity-based infrastructure, the proposed frameworks enhance real-time detection accuracy and scalability, effectively addressing IoT-specific vulnerabilities. The integration of ML models enables the identification of complex threat patterns, making the approach suitable for dynamic and evolving IoT landscapes. However, the study primarily focuses on intrusion detection and does not delve into layered or centralized security strategies, which are essential for

comprehensive protection in MEC systems. This gap highlights the need for broader frameworks that integrate multiple security layers to address the diverse challenges of MEC-enabled IoT ecosystems[5].

The review on MEC Architecture and Security provides an in-depth analysis of the vulnerabilities inherent in MEC systems and emphasizes the importance of layered security controls and centralized architectures to mitigate potential attacks. By proposing solutions such as distributed nodes and scalable access control mechanisms, the study highlights effective strategies to enhance data integrity and system resilience. The layered approach is particularly valuable for addressing diverse security threats in MEC environments. However, the review primarily focuses on architectural design and theoretical solutions, offering limited exploration of dynamic threat detection mechanisms or real-time security implementations. This limitation underscores the need for practical frameworks that integrate advanced threat detection and response capabilities alongside robust architectural safeguards[6]. The first study leverages knowledge distillation and transfer learning to develop lightweight, efficient anomaly detection models, enhancing scalability and detection accuracy in resource-constrained MEC environments. The second paper focuses on machine learning-enhanced Network Intrusion Detection Systems (NIDS), utilizing MEC's low-latency infrastructure to achieve real-time detection of IoT-specific threats. Lastly, the survey provides a comprehensive analysis of MEC security and privacy frameworks, emphasizing layered architectures and privacy-preserving measures to mitigate attack vectors and ensure data integrity. While these studies offer valuable insights into improving MEC security, they highlight gaps such as the need for holistic frameworks that integrate anomaly detection, intrusion prevention, and robust encryption mechanisms to address the complex threat landscape comprehensively[7].

3. Methodologies

3.1 Adaptive Risk-Aware Resource Orchestration for 5G Microservices:

The methodology presented in Adaptive Risk-Aware Resource Orchestration for 5G Microservices offers an innovative approach to managing resources in MEC environments. At its core, the framework employs probabilistic risk assessment to evaluate the potential threats and inefficiencies associated with resource allocation in real-time. This dynamic model ensures efficient resource distribution by prioritizing critical applications and mitigating the impact of malicious processes, thereby enhancing system resilience and reducing latency—a crucial factor for time-sensitive applications. The adaptive, real-time nature of the framework allows it to respond quickly to changes in the network environment, such as fluctuating resource demands or newly detected threats, ensuring optimized performance and scalability across multi-tier edge-cloud systems. Despite its strengths, the methodology focuses primarily on resource management and does not address broader security mechanisms. It lacks integration with advanced authentication protocols, real-time intrusion detection systems, or comprehensive data encryption methods, which are essential for a holistic MEC security framework. While the framework significantly improves resource utilization and system performance, future enhancements could incorporate additional layers of security to create a more robust and secure MEC solution. This methodology demonstrates a strong foundation for addressing resource allocation challenges but leaves room for further development to meet the full spectrum of MEC security needs[1].

Algorithm 1 Resource Allocation and Performance Optimization

Initialization:
Initialize L_m and A_m for all m
Set stopping criterion ϵ
while change in objective $> \epsilon$ **do**
  Step 1: Optimize Resource Allocation and Function Placement
  for each application m **do**
    Fix L_m and A_m
    Solve resource allocation problem
    Update $r_{v,m}^{\text{com}}$, $r_{v,m}^{\text{net}}$, and $x_{v,m}^{n}$
  end for
  Step 2: Update Performance Metrics
  for each application m **do**
    Determine new L_m and A_m
    Update L_m and A_m in the optimization problem
  end for
  Step 3: Update Objective Function
  Compute new objective value
  Check for convergence
end while

Figure 1. Algorithm Implemented [1].

3.2 Attribute-Based Management for Secure Kubernetes Cloud Bursting

The methodology proposed by Femminella et al. in Attribute-Based Management for Secure Kubernetes Cloud Bursting focuses on enhancing security for Kubernetes-based cloud bursting operations through

the integration of Attribute-Based Encryption (ABE). This innovative approach addresses the critical need for secure, scalable, and privacy-compliant resource management in distributed MEC environments. At the core of the methodology is the use of ABE, which provides fine-grained access control by granting permissions based on specific attributes such as user roles, resource requirements, or organizational policies. This ensures that access to resources is tightly controlled and restricted to authorized entities, significantly reducing the risk of unauthorized access or data breaches. Additionally, the framework enhances Kubernetes' labeling system, enabling dynamic security policies that can adapt in real-time to changes in workloads or user attributes. This flexibility makes it particularly well-suited for environments where resource demands and user access requirements are constantly evolving. The methodology ensures scalability, allowing security measures to expand alongside increasing workloads without compromising performance. Furthermore, it aligns with privacy regulations, making it ideal for scenarios where sensitive data must be securely managed during cloud bursting operations, which involve the transfer of workloads between private and public clouds. Despite these strengths, the methodology is limited in scope. While it effectively secures access control and resource allocation, it does not address broader security needs such as anomaly detection, real-time threat mitigation, or advanced encryption beyond access control. These gaps highlight the need for further integration with complementary security measures to create a holistic MEC security framework. In conclusion, this methodology provides a robust solution for secure resource orchestration in Kubernetes environments. Its focus on ABE and dynamic policy enforcement makes it highly effective for privacy-compliant and scalable operations. However, future research could enhance its applicability by incorporating broader security mechanisms, such as intrusion detection and real-time threat response, to address the full spectrum of security challenges in MEC ecosystems[2].

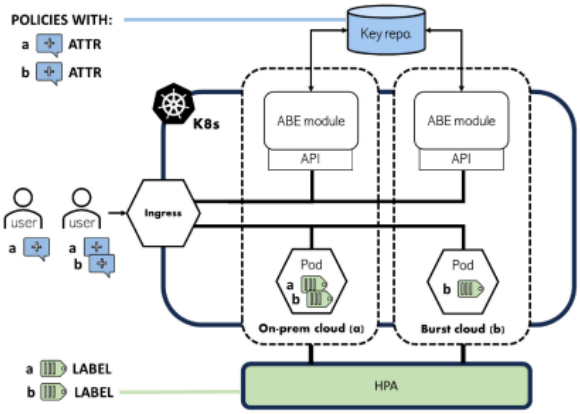

Figure 2. High-level diagram that illustrates the primary stakeholders and their interconnections of our model[2].

3.3 Efficient Authentication in Cloud-Fog-Device Frameworks

The methodology outlined in Efficient Authentication in Cloud-Fog-Device Frameworks presents a robust solution for addressing authentication challenges in resource-constrained cloud-fog-device ecosystems. By leveraging elliptic curve cryptography (ECC) and cryptographic hashing, the framework ensures secure, lightweight, and efficient authentication suitable for distributed environments like MEC. The use of ECC is central to this methodology, offering strong encryption with smaller key sizes compared to traditional methods such as RSA. This ensures high levels of security while reducing computational overhead, making it ideal for fog and IoT devices with limited processing power. Cryptographic hashing further strengthens the authentication process by maintaining data integrity and protecting against tampering or replay attacks. A key feature of this framework is its emphasis on key agreement and management protocols, which enable secure establishment, distribution, and renewal of cryptographic keys among cloud, fog, and device layers. These protocols address vulnerabilities such as key-revelation attacks, ensuring that a single compromised key does not compromise the entire system. Despite its strengths, the methodology is focused exclusively on authentication and does not extend to other critical security measures. For instance, it lacks integration with intrusion detection systems for identifying unauthorized access or malicious activities. Additionally, while ECC is used for secure key exchange, the framework does not provide comprehensive data encryption solutions for securing data during storage or transmission. In conclusion, this methodology offers an

efficient and secure authentication mechanism that is particularly suited for environments with constrained resources. However, expanding its scope to include broader security measures, such as real-time threat detection and layered encryption, would significantly enhance its utility for comprehensive MEC ecosystem security[3].

3.3.1 Elliptic Curve Cryptography (ECC):

This methodology leverages ECC for secure key generation and exchange. ECC provides strong encryption with smaller key sizes, ensuring robust security while minimizing computational costs. This makes it particularly suitable for resource-constrained environments such as fog and IoT devices, where processing power is limited. ECC is used throughout the framework to establish secure communication channels between devices, fog nodes, and cloud servers.

3.3.2 Cryptographic Hash Functions:

The framework incorporates cryptographic hash functions to enhance data integrity and ensure that transmitted data cannot be tampered with. Hashing is employed during key exchange and authentication to validate the freshness and integrity of messages, mitigating the risk of replay and forgery attacks.

3.3.3 Key Agreement and Management:

A significant focus of the methodology is on secure key agreement protocols that enable devices and servers to establish shared secret keys over insecure communication channels. The framework ensures that keys are securely generated, exchanged, and stored. Key management also includes periodic renewal to maintain security and resilience against attacks such as key-revelation.

3.3.4 Mutual Authentication:

The methodology ensures mutual authentication between all entities in the cloud-fog-device ecosystem, including users, devices, fog nodes, and cloud servers. By verifying the identities of all participants during communication, the framework reduces the risk of impersonation and unauthorized access.

3.3.5 Lightweight Design:

Designed to be computationally efficient, the methodology minimizes resource consumption while maintaining robust security. This lightweight design ensures compatibility with IoT devices and fog nodes that have limited processing power and energy constraints.

3.3.6 Formal Security Verification:

The framework undergoes rigorous security analysis using models such as the Real-Or-Random (ROR) model and Scyther tool to confirm its resilience against various attacks, including replay, man-in-the-middle, and key-revelation attacks. This verification ensures that the methodology meets the security requirements of modern MEC ecosystems.

3.4 Efficient Anomaly Detection for Edge Clouds

The methodology outlined in the paper focuses on addressing the dual challenges of resource constraints and limited labeled data in edge cloud environments. It employs transfer learning and knowledge distillation to develop lightweight, efficient anomaly detection models. Below is a categorized summary:

3.4.1 Transfer Learning:

Transfer learning is used to leverage knowledge from a pre-trained model trained on a large dataset from a related domain.

- Pre-Trained Model Utilization: A pre-trained model is trained on a larger dataset (e.g., intrusion detection datasets) to learn general patterns.
- Domain Adaptation: The knowledge from the pre-trained model is fine-tuned to smaller, edge cloud-specific datasets with limited labeled data. This reduces the need for extensive data collection and training on edge datasets while retaining high detection accuracy.
- Applicability to Model Types: Transfer learning is applied to both sequential (e.g., LSTM, GRU) and non-sequential models (e.g., ANN) to enhance performance across varying types of data[4].

3.4.2 Knowledge Distillation:

Knowledge distillation compresses the knowledge of a larger, complex "teacher model" into a smaller, more efficient "student model."

- Teacher-Student Framework: The teacher model, trained on a larger dataset, provides soft labels or probabilistic outputs to guide the student model's training.
- Lightweight Student Model: The student model is designed to mimic the teacher model's capabilities

while being computationally efficient, making it suitable for resource-constrained edge environments.

- Efficiency Gains: The distillation process reduces detection time and computational overhead while maintaining a high level of anomaly detection accuracy.[4]

3.4.3 Hybrid Architecture Support:

The methodology supports both sequential and non-sequential model architectures.

- Non-Sequential Models (ANN): Ideal for feature-based anomaly detection tasks without temporal dependencies.
- Sequential Models (LSTM, GRU): Suitable for detecting anomalies in time-series data by capturing temporal dependencies.[4]

3.4.4 Model Optimization and Training:

- Training Process: Models are trained initially on large datasets and fine-tuned for edge-specific datasets.
- Layer Freezing: In non-sequential models, the initial layers are frozen during fine-tuning to retain learned features while adapting higher layers for domain-specific tasks.
- Distillation Loss: Knowledge distillation incorporates a loss function, typically Kullback-Leibler divergence, to align the student model's predictions with the teacher's outputs[4].

Algorithm 1 Transfer Learning With Knowledge Distillation for Non-Sequential Model (ANN)

Require: Large dataset D_{large}, Small dataset D_{small}, Larger model f_{ANN},
Distillation weight α, Temperature T, Optimizer O, Student_loss_fn L_s,
Distillation_loss_fn L_d, Epochs E, Batch_size B, Number of frozen layers K

1: Initialize parameters θ_{ANN}, θ_{small}
2: Train f_{ANN} on D_{large} using backpropagation and optimization algorithm specified by O
3: Freeze the first K layers of f_{ANN} and obtain θ_{freeze}
4: Fine-tune the remaining layers of f_{ANN} on D_{small} for E epochs with batch size B and obtain $\theta_{\text{fine-tune}}$
5: Compute soft targets $\mathbf{q} = P(\mathbf{y}_{\text{Large}})$ using θ_{freeze} and $\theta_{\text{fine-tune}}$ with temperature T
6: Train f_{small} on D_{small} using $\mathbf{q}$ as soft targets via minimizing L_d and L_s weighted by α
7: **return** $f_{\text{ANN}}, f_{\text{small}}$

Algorithm 2 Transfer Learning With Knowledge Distillation for Sequential Models (LSTM/GRU)

Require: Large dataset D_{large}, Small dataset D_{small}, Larger model $f_{\text{LSTM/GRU}}$,
Distillation weight α, Temperature T, Optimizer O, Student_loss_fn L_s,
Distillation_loss_fn L_d, Epochs E, Batch_size B, Number of frozen layers K

1: Initialize parameters $\theta_{\text{LSTM/GRU}}$
2: Train $f_{\text{LSTM/GRU}}$ on D_{large} using backpropagation and optimization algorithm specified by O for E epochs with batch size B
3: Retrain $f_{\text{LSTM/GRU}}$ on D_{small} using backpropagation and optimization algorithm specified by O for E epochs with batch size B
4: Compute soft targets $\mathbf{q} = P(\mathbf{y}_{\text{Large}})$ with temperature T
5: Train a smaller sequential model f_{small} on D_{small} using $\mathbf{q}$ as soft targets via minimizing L_d and L_s weighted by α
6: **return** $f_{\text{LSTM/GRU}}, f_{\text{small}}$

The methodology outlined in Efficient Anomaly Detection for Edge Clouds provides an innovative approach to addressing anomaly detection challenges in resource-constrained MEC environments. It employs knowledge distillation and transfer learning to create lightweight yet effective models that maintain high accuracy while optimizing computational efficiency. Knowledge distillation is a core component of this approach. In this technique, a large, complex "teacher" model is trained to achieve high anomaly detection accuracy. The knowledge and insights learned by this teacher model are then transferred to a smaller, more efficient "student" model. This transfer process ensures that the student model retains the detection capabilities of the teacher while being lightweight enough to operate on devices with limited computational resources, such as IoT devices or edge nodes. Transfer learning complements this by reducing the dependency on extensive training datasets. It leverages pre-trained models from similar tasks or datasets, allowing the anomaly detection system to adapt to new environments or evolving threats with minimal retraining. This makes the methodology particularly scalable and suitable for dynamic MEC systems, where data availability and computational capacity vary. The combined use of these techniques results in models that are computationally efficient, scalable, and capable of achieving high detection accuracy in distributed edge environments. These lightweight models are ideal for MEC infrastructures where limited processing power, memory, and network bandwidth are common constraints. However, the

methodology is focused solely on anomaly detection and does not incorporate broader security measures, such as encryption for data protection, intrusion detection for comprehensive threat management, or real-time response mechanisms. Expanding the scope to include these elements would enhance the methodology's applicability to holistic MEC security frameworks. In summary, this methodology effectively balances performance and resource efficiency, making it a valuable tool for anomaly detection in MEC systems. Its use of knowledge distillation and transfer learning ensures scalability and adaptability, but integrating additional security measures would make it more robust and comprehensive.[4]

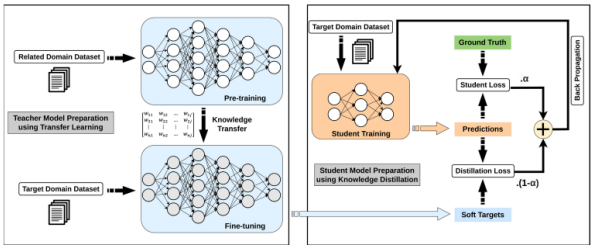

Figure 3. The schema of the proposed approach[4].

3.5 Intrusion Detection in IoT Systems

The methodology outlined in Intrusion Detection in IoT Systems integrates machine learning (ML) algorithms with MEC-enabled Network Intrusion Detection Systems (NIDS) to address IoT-specific security challenges. This approach leverages MEC's low-latency, proximity-aware architecture to provide real-time and scalable intrusion detection, making it particularly effective in dynamic and distributed IoT environments. The system utilizes advanced ML algorithms, such as decision trees and neural networks, to analyze network traffic and detect suspicious activity. These algorithms are capable of identifying complex and evolving threat patterns, including those specific to IoT devices, such as DDoS attacks or malware propagation. By training on historical data and adapting to new attack vectors, the ML-based NIDS ensures high detection accuracy and adaptability to emerging threats. The integration with MEC infrastructure enables the NIDS to process data at the network edge, significantly reducing latency compared to centralized cloud-based solutions. This proximity-based analysis ensures faster threat detection and response, enhancing the overall security posture of IoT ecosystems. Additionally, the system is designed to scale efficiently, accommodating the increasing number of IoT devices and their associated data flows. Despite its strengths, the methodology focuses narrowly on intrusion detection and lacks broader security measures. It does not incorporate layered security strategies, such as combining intrusion detection with encryption or privacy-preserving techniques, which are essential for comprehensive protection. Additionally, the absence of real-time threat response mechanisms limits its ability to mitigate detected intrusions automatically. In summary, this methodology provides an efficient and scalable solution for IoT-specific intrusion detection by combining ML with MEC's low-latency capabilities. While it excels in real-time threat analysis, expanding its scope to include multi-layered defenses, encryption, and automated response mechanisms would significantly enhance its effectiveness as a holistic security framework for MEC-enabled IoT systems[5].

3.6 MEC Architecture and Security

The methodology described in MEC Architecture and Security emphasizes a layered security architecture to address the unique vulnerabilities of MEC environments. This approach combines distributed nodes and centralized control mechanisms to create a robust framework that ensures data integrity and defends against unauthorized access and potential breaches. A key component of this methodology is the use of scalable access control policies, which allow the system to dynamically adjust permissions based on user roles, device attributes, or network conditions. This scalability ensures that security remains effective even as the number of connected devices and data flows in MEC environments continues to grow. The layered architecture divides the security responsibilities across multiple tiers, reducing the impact of a single point of failure and making the overall system more resilient. The distributed node architecture plays a vital role in decentralizing computational tasks, improving fault tolerance, and enhancing data confidentiality by keeping sensitive information closer to the edge. At the same time, centralized control mechanisms provide overarching management and coordination, ensuring that security policies are consistently applied across the network. While the layered approach strengthens the overall security posture and enhances system resilience, the methodology primarily focuses on theoretical guidelines. It does not integrate dynamic threat detection mechanisms or real-time response systems, which are crucial for identifying and mitigating evolving cyber threats. This limitation reduces its

practical applicability in environments where real-time security measures are essential[6].

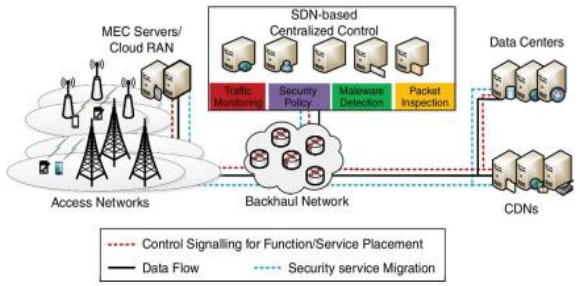

Figure 4. Centralized Security Architecture for MEC[6]

The methodology employs a layered security framework to address MEC vulnerabilities by distributing responsibilities across multiple tiers, reducing single points of failure. It includes:

- **Scalable Access Control:** Dynamic policies based on user roles, device attributes, or network conditions to manage permissions effectively as device numbers grow.
- **Distributed Node Architecture:** Decentralized computation to enhance fault tolerance and keep sensitive data closer to the edge, reducing transmission risks.
- **Centralized Control Mechanisms:** Uniform management and enforcement of security policies for consistency and resource optimization.
- **Data Integrity Measures:** Use of cryptographic hashing and secure protocols to prevent unauthorized data modifications.[6]

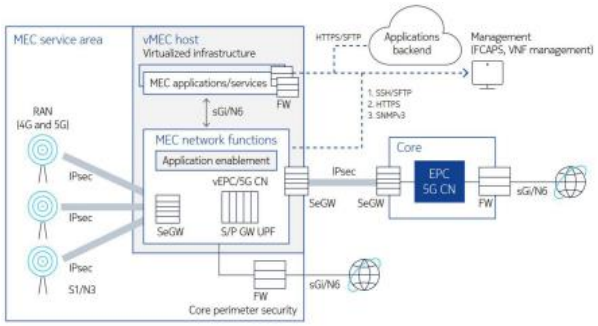

Figure 5. MEC Security Network Architecture[6].

3.7 Machine Learning-Based Intrusion Detection Systems (NIDS):

The Machine Learning-Based Intrusion Detection Systems (NIDS) methodology integrates advanced machine learning (ML) algorithms into MEC-enabled NIDS frameworks to bolster security in IoT networks. This approach utilizes ML techniques such as decision trees and neural networks to analyze network traffic and identify intrusion patterns effectively. These algorithms enable the system to detect both known and emerging threats, making it highly adaptable to evolving attack landscapes. By leveraging the low-latency, proximity-aware infrastructure of MEC, this methodology ensures real-time threat detection and rapid response, a critical feature for dynamic and time-sensitive IoT environments where security breaches need immediate attention. The ML-based NIDS is particularly effective against complex attack vectors, including Distributed Denial of Service (DDoS) attacks and malware propagation. The system's ability to learn from historical data and adapt to new threats enhances its detection accuracy and reliability. Furthermore, its scalable design allows it to accommodate the ever-growing number of IoT devices and their associated data flows, ensuring robust performance in large-scale deployments. Despite its strengths, this methodology focuses narrowly on intrusion detection and lacks broader security measures. It does not incorporate multi-layered defenses or encryption mechanisms to safeguard data during transmission and storage. These gaps leave certain vulnerabilities unaddressed, particularly in scenarios requiring comprehensive protection. Expanding the framework to include automated threat response systems, layered security architectures, and advanced data encryption could provide a more holistic security solution for MEC environments. Such enhancements would ensure that the methodology not only detects intrusions effectively but also mitigates risks and protects sensitive data against a wide range of cyber threats.

4. Results

The combined analysis, highlights the transformative potential of integrating Security as a Service (SecaaS) with Multi-Access Edge Computing (MEC) infrastructure to address modern cybersecurity challenges. MEC's decentralized, low-latency, and proximity-aware design provides a robust platform for securing distributed systems, particularly IoT networks and real-time applications. The reviewed studies emphasize the adoption of advanced methodologies such as knowledge distillation, transfer learning, machine learning-based intrusion detection systems (NIDS), and layered security architectures. Knowledge distillation and transfer learning are instrumental in creating lightweight anomaly detection models that

optimize resource-constrained environments, while ML-enhanced NIDS frameworks significantly improve detection rates and accuracy for IoT-specific threats[5]. Additionally, layered security architectures integrate distributed and centralized controls to strengthen defenses against data breaches while maintaining system scalability. A comparative analysis reveals that MEC's architecture enhances security scalability and responsiveness, addressing issues like resource constraints and dynamic threat vectors[7]. Adaptive resource orchestration and encryption mechanisms provide additional layers of security, while advanced authentication protocols safeguard edge-cloud-device frameworks against vulnerabilities such as key-revelation attacks. The findings underscore the need for a unified SecaaS-MEC framework that combines adaptive resource allocation, AI-driven analytics, and robust encryption to deliver comprehensive security solutions for edge environments. This integration not only mitigates evolving cyber threats but also ensures operational efficiencies, low latency, and enhanced real-time responsiveness. Future research should focus on further leveraging AI and advanced cryptographic techniques to refine SecaaS platforms for diverse MEC applications[1].

The results of the reviewed methodologies highlight significant advancements in performance, security, and reliability within SecaaS-MEC frameworks. In terms of performance and scalability, transfer learning emerges as a pivotal technique, effectively reducing dependency on extensive training data and enabling the development of lightweight models suitable for resource-constrained environments. Adaptive orchestration models further optimize resource utilization, enhancing system responsiveness and ensuring efficient operations in dynamic edge-cloud scenarios. From a security perspective, Attribute-Based Encryption (ABE) and centralized security architectures provide robust mechanisms to safeguard data confidentiality and ensure compliance with privacy regulations[2]. Additionally, machine learning-based intrusion detection systems (IDS) demonstrate notable improvements in detecting and mitigating threats in real-time applications, particularly in IoT ecosystems. Lastly, advanced authentication schemes exhibit high reliability, showcasing resilience to evolving threats and effectively addressing resource constraints in edge networks. These results collectively underscore the potential of integrating MEC with SecaaS to achieve scalable, secure, and adaptive cybersecurity solutions.

Table 1: Comparative Analysis of Results

Aspect	**Adaptive Resource Orchestration**[1], [2], [3]	**Knowledge Distillation & Transfer Learning** [4],[5],[6]	**Layered Security Architectures**[7]
Focus	Integration of SecaaS with MEC for scalable security	SecaaS leveraging MEC for IoT and anomaly detection	SecaaS for IoT security and privacy in MEC environments
Key Methodologies	Adaptive resource orchestration	Knowledge distillation	Knowledge distillation
	Attribute-Based Encryption (ABE)	Transfer learning	Transfer learning
	Advanced authentication protocols	Hybrid NIDS frameworks	Layered security architectures
Target Challenges	Latency-sensitive security, scalable authentication	IoT-specific anomaly detection, resource constraints	Threat vectors in MEC, IoT anomaly detection, privacy frameworks
Performance Metrics	Improved resource utilization	Reduced training data dependency	Enhanced threat detection accuracy
	Enhanced latency	Improved anomaly detection rates	Scalability and privacy in MEC architectures
	Scalable authentication		

Aspect	**Adaptive Resource Orchestration**[1], [2], [3]	**Knowledge Distillation & Transfer Learning** [4],[5],[6]	**Layered Security Architectures**[7]
Results	Enhanced MEC resilience with dynamic allocation	Lightweight models effective for edge anomaly detection	Superior NIDS performance in detecting IoT-specific threats
	Robust encryption and authentication	Higher detection accuracy in IoT systems	Centralized and distributed controls for scalability
Strengths	Comprehensive integration of SecaaS with MEC	Efficient anomaly detection for resource-limited environments	Decentralized design for low latency
	Real-time adaptability	Strong IoT focus	Effective mitigation of MEC-specific vulnerabilities
Limitations	Lacks holistic integration across methodologies	Focused primarily on IoT scenarios	Centralized control may limit some MEC decentralization benefits
Future Directions	Unified SecaaS-MEC framework with AI-driven analytics	AI-enhanced analytics for broader SecaaS-MEC applications	Advanced cryptographic techniques and AI for secure MEC environments

5. Conclusion

This infrastructure presents a transformative solution to modern cybersecurity challenges, particularly in IoT and edge network environments. Leveraging MEC's distributed, low-latency architecture enables enhanced security scalability, real-time responsiveness, and optimized resource utilization. However, existing frameworks lack a holistic approach to integrating adaptive orchestration, robust encryption, and secure authentication. Future advancements should focus on developing unified SecaaS-MEC models that incorporate AI-driven analytics and advanced cryptographic techniques to address evolving threat vectors. This integration will not only enhance security resilience but also ensure compliance with privacy regulations and support the scalability needed for dynamic edge-cloud ecosystems. Additionally, the future scope includes exploring lightweight AI models and privacy-preserving mechanisms to further optimize SecaaS for resource-constrained environments and next-generation network applications.

References

[1] X. Wu, J. Farooq, and J. Chen, “Adaptive Risk-Aware Resource Orchestration for 5G Microservices over Multi-Tier Edge-Cloud Systems,” Jun. 12, 2024. doi: 10.36227/techrxiv.171822324.47913612/v1.

[2] M. Femminella, M. Palmucci, G. Reali, and M. Rengo, “Attribute-Based Management of Secure Kubernetes Cloud Bursting,” *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1276–1298, 2024, doi: 10.1109/OJCOMS.2024.3367461.

[3] M. Hegde, R. R. Rao, and R. Bhat, “Design of an Efficient and Secure Authentication Scheme for Cloud-Fog-Device Framework Using Key Agreement and Management,” *IEEE Access*, vol. 12, pp. 78173–78192, 2024, doi: 10.1109/ACCESS.2024.3407103.

[4] J. Forough, H. Haddadi, M. Bhuyan, and E. Elmroth, “Efficient Anomaly Detection for Edge Clouds: Mitigating Data and Resource Constraints,” *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3492815.

[5] E. Gyamfi and A. Jurcut, “Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets,” May 01, 2022, *MDPI*. doi: 10.3390/s22103744.

[6] B. Ali, M. A. Gregory, and S. Li, “Multi-access edge computing architecture, data security and privacy: A review,” 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3053233.

[7] P. Ranaweera, A. D. Jurcut, and M. Liyanage, “Survey on Multi-Access Edge Computing Security and Privacy,” Apr. 01, 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/COMST.2021.3062546