International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

An Integrated Framework for Security Policy Management in Cloud and Edge Computing Environments

Bhawana Parihar[1], Dr. Poonam Chimmwal[2]

[1]Assistant Professor, Computer Science and Engineering Department, Bipin Tripathi Kumaon Institute of Technology, Dwarahat Distt Almora, Uttarakhand 263653,

dr.bhawanaparihar@gmail.com

[2]Assistant Professor, Computer Science and Engineering Department, Bipin Tripathi Kumaon Institute of Technology, Dwarahat Distt Almora, Uttarakhand 263653,

poonamwise@gmail.com, Corresponding author mail: dr.bhawanaparihar@gmail.com

Abstract: The integration of cloud and edge computing technologies has revolutionized modern IT infrastructures by providing enhanced scalability, flexibility, and lower latency for data processing. However, the hybrid nature of these environments introduces unique security challenges, particularly in managing security policies across both centralized cloud systems and decentralized edge nodes. This paper presents an integrated framework for security policy management in cloud and edge computing environments, aimed at addressing the complex and evolving security requirements of these interconnected systems. The proposed framework combines classical security techniques with advanced methodologies such as machine learning-based threat detection, lightweight cryptography for IoT devices, and dynamic policy enforcement mechanisms. It focuses on critical areas such as identity and access management, secure communication, data privacy, and real-time monitoring of security events. By employing an adaptive approach to policy management, the framework ensures that security measures can respond in real-time to emerging threats while optimizing resource use across cloud and edge nodes. Additionally, the framework supports the seamless integration of cloud and edge-specific security models, offering a scalable, efficient, and future-proof solution to securing hybrid environments. The paper also discusses potential challenges and future advancements required to enhance security policy management in cloud-edge ecosystems, paving the way for robust, secure, and resilient infrastructures.

Keywords*:* Cloud Computing, Edge Computing, Security Policy Management, Data Privacy, Access Control, Identity Management, Threat Detection, Machine Learning, Cryptography, IoT Security, Real-time Monitoring, Hybrid Environments, Dynamic Policy Enforcement.

1. Introduction

Cloud computing and edge computing are two complementary technologies that have transformed the way enterprises and service providers deliver computing services. While **cloud computing** has revolutionized the IT industry by offering scalable, on-demand resources over the internet, **edge computing** extends this model by providing data processing and storage capabilities closer to the data source, such as IoT devices and sensors. Together, these technologies form a hybrid architecture, often referred to as the **cloud-edge ecosystem**, which provides significant benefits in terms of latency reduction, bandwidth optimization, and improved service delivery. However, the integration of cloud and edge computing presents new and complex security challenges that need to be addressed to ensure the protection of sensitive data, resources, and communication channels across these distributed systems[1].

In a cloud-edge ecosystem, security management must consider the unique characteristics of both paradigms. The **cloud** is a centralized environment where large-scale data storage, computational power, and networking resources are provided by third-party service providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. Security policies in the cloud primarily focus on data protection, identity and access management (IAM), encryption, and network security. However, the edge layer consists of distributed devices and nodes located at the edge of the network, close to the data source. These devices are typically constrained in terms of computational power,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

memory, and energy resources, which makes implementing traditional security measures challenging[2].

Moreover, the dynamic nature of cloud-edge systems introduces additional complexities. Security policies that work well in a centralized cloud environment may not be directly applicable to decentralized edge devices. Edge nodes often operate in diverse, untrusted environments, which increases the attack surface and vulnerability to cyber threats. Therefore, managing security policies in a hybrid cloud-edge system requires a flexible, scalable, and adaptive framework that can handle both centralized and distributed security management.

Security Challenges in Cloud and Edge Environments

One of the most significant challenges in managing security in cloud and edge environments is ensuring **data privacy**. In cloud computing, data privacy is often achieved through encryption, access control mechanisms, and data segmentation. However, when data is transferred between cloud and edge devices, ensuring the security of data in transit becomes critical. Edge devices, being closer to end users, collect and process large volumes of data, often including sensitive information. Ensuring that data privacy is maintained at both the cloud and edge layers is vital for protecting user privacy and meeting regulatory compliance standards such as **GDPR** (General Data Protection Regulation) and **HIPAA** (Health Insurance Portability and Accountability Act)[3,4].

Another key concern is **access control**. In cloud environments, managing who can access specific resources is done using **IAM policies**, which define user roles, permissions, and authentication mechanisms. However, edge devices present a unique challenge in this regard due to their decentralized nature. Edge devices may be located in remote or untrusted environments, making them vulnerable to physical tampering or unauthorized access. Moreover, users and devices may need to interact with both cloud and edge resources, requiring seamless and secure cross-platform access control policies.

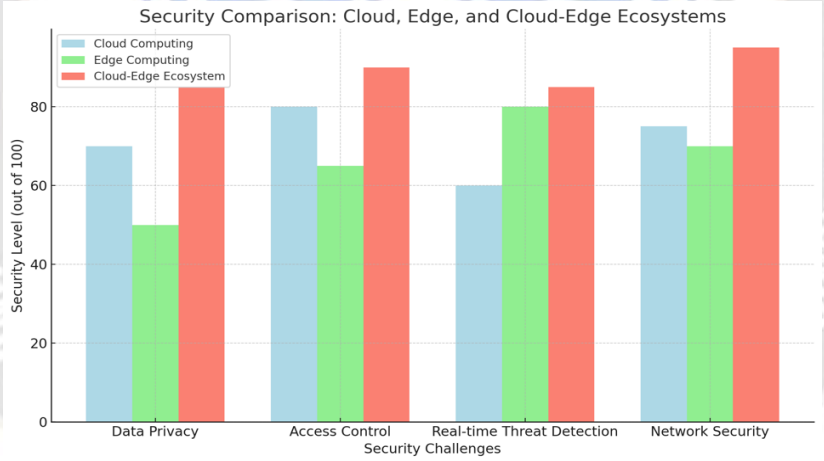

Figure 1: Security Comparison: Cloud, Edge, And Cloud-Edge Ecosystems

Furthermore, **real-time threat detection** is a critical aspect of security in cloud-edge ecosystems. Both cloud and edge layers are susceptible to a variety of cyber-attacks, such as **Distributed Denial of Service (DDoS)** attacks, **data breaches**, and **man-in-the-middle** attacks. In the cloud, large-scale anomaly detection systems can monitor and analyze network traffic, user behavior, and resource utilization to detect potential threats[5]. However, the decentralized and dynamic nature of edge devices makes real-time threat detection more complex. Edge devices must be able to detect and respond to threats locally without relying on constant communication with the cloud, thus ensuring resilience even in the absence of a stable connection.

A promising solution to these challenges lies in the development of an **integrated security policy management framework**. This framework must be capable of adapting to the security needs of both cloud and edge systems, providing comprehensive protection for data, resources, and communication. Such a framework would combine traditional security measures with emerging technologies, such as **machine learning (ML)** and **lightweight cryptography**, to enhance the detection and mitigation of threats across hybrid environments[6,7].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

Table 1: Key Security Challenges in Cloud and Edge Computing Environments

Security Challenge	Cloud Computing	Edge Computing
Data Privacy	Ensuring data encryption, access control, and compliance with regulations like GDPR	Protecting data at rest, in transit, and on edge devices, especially sensitive data such as personal information
Access Control	Centralized IAM policies, multi-factor authentication, encryption	Distributed access control, secure device authentication, dynamic policy enforcement
Real-Time Threat Detection	Cloud-based anomaly detection, large-scale threat monitoring	Local threat detection on edge devices, real-time response with limited resources
Network Security	Securing communication between cloud resources, VPNs, firewalls	Securing communication between edge nodes and the cloud, encryption of edge data transmissions

Proposed Framework for Security Policy Management

To address the security challenges in cloud and edge computing environments, we propose an integrated security policy management framework that combines both centralized and decentralized security models. The framework integrates several key components:

1. **Identity and Access Management (IAM)**: A robust IAM system is essential for controlling user and device access to cloud and edge resources. The framework employs **multi-factor authentication (MFA)** and **role-based access control (RBAC)** to ensure that only authorized users and devices can access sensitive resources. The framework also supports **dynamic access control** based on real-time contextual information, such as the location of edge devices or the state of the network connection.

2. **Data Privacy and Encryption**: The framework ensures data privacy by employing **end-to-end encryption** for data transferred between the cloud and edge devices. It also integrates **lightweight cryptographic protocols**, such as **PRESENT** and **TEA**, to provide secure encryption for IoT devices with limited computational resources. These protocols ensure that data remains confidential and protected from unauthorized access or tampering.

3. **Real-Time Threat Detection and Response**: The framework uses **machine learning-based anomaly detection** algorithms to monitor network traffic, device behavior, and user interactions in real-time. By leveraging **AI-based threat intelligence**, the framework can detect abnormal activities, such as DDoS attacks or data exfiltration attempts, and respond dynamically. Additionally, **edge devices** can autonomously mitigate threats, such as isolating compromised devices or triggering local alarms, without waiting for cloud intervention.

4. **Policy Enforcement and Monitoring**: The framework employs a **distributed policy enforcement mechanism** that operates both in the cloud and at the edge. Policies are defined centrally in the cloud and then propagated to the edge devices for local enforcement. The framework also provides continuous monitoring and auditing capabilities to ensure compliance with security policies, detect policy violations, and generate detailed logs for forensic analysis.

The hybrid cloud-edge computing architecture presents unique challenges in terms of security management. Ensuring data privacy, implementing effective access control, detecting real-time threats, and maintaining robust network security are all critical aspects that must be addressed. The proposed integrated security policy management framework provides a comprehensive solution by combining centralized and decentralized security mechanisms, enabling seamless protection across cloud and edge environments. By leveraging advanced techniques such as machine learning and lightweight cryptography, the framework ensures scalable, efficient, and adaptive security measures that can respond to both current and emerging threats. Future work will focus on optimizing the framework for large-scale deployment and enhancing its ability to handle more complex security scenarios in dynamic, real-world cloud-edge ecosystems.

2. Related Work

Cloud computing and edge computing have emerged as two of the most transformative technologies in modern IT infrastructure. These technologies offer several benefits, including **scalability**, **low latency**, and **improved service delivery**. While **cloud computing** has revolutionized data storage, computation, and resource sharing, **edge computing** brings computational power closer to the data source, providing faster processing and reducing bandwidth

consumption. By distributing data processing tasks across multiple devices, edge computing can mitigate some of the limitations of cloud computing, particularly in terms of latency and bandwidth. However, the integration of these two paradigms introduces unique security challenges that need to be addressed for a secure and robust cloud-edge ecosystem. In this section, we explore the existing body of work that addresses these security challenges, focusing on the management of security policies in hybrid cloud-edge environments.

Cloud and Edge Computing Security Challenges

Security is one of the most critical aspects of cloud and edge computing. While both cloud and edge computing share some common security concerns, such as **data privacy**, **access control**, and **network security**, the distributed and decentralized nature of edge computing introduces additional complexities. Cloud environments are typically centralized, where data and resources are managed by a service provider, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud[8]. These centralized environments make it easier to apply security measures such as **identity and access management (IAM)**, **encryption**, and **firewalls**. However, edge computing environments introduce a more distributed architecture, where data is processed on devices located at or near the data source, often in untrusted and dynamic environments[9].

A key challenge is ensuring **data privacy** in a cloud-edge ecosystem. In the cloud, data privacy is managed through encryption and access controls that limit who can view and manipulate sensitive data. However, when data is transferred between the cloud and edge nodes, ensuring its protection during transmission is critical. Edge devices, which often handle sensitive data such as personal information or health-related data, must implement strong encryption and privacy-preserving techniques to prevent unauthorized access or data breaches. The use of **lightweight cryptographic protocols**, such as **PRESENT** and **TEA**, is emerging as an effective solution to maintain data privacy in the context of resource-constrained edge devices.

Another significant challenge in cloud-edge ecosystems is **access control**. While cloud environments rely on IAM systems to manage access to resources, edge devices are much more diverse, and managing access control in such an environment is more difficult. Edge devices often have limited processing power and storage, making traditional IAM systems impractical. Therefore, **dynamic access control mechanisms** are required that can adapt to the changing nature of edge devices. For example, access control policies should be able to change based on the location of the edge device, its current status, and the type of data being processed. This requires the integration of flexible, **context-aware access control mechanisms** that can enforce security policies based on real-time information[10].

Moreover, **real-time threat detection** is critical in both cloud and edge environments. In the cloud, large-scale anomaly detection systems can monitor and analyze network traffic, user behavior, and resource usage to detect potential threats. However, real-time threat detection at the edge is more challenging due to the limited computational resources and the physical distribution of devices. Since edge devices are often deployed in remote locations, they may not have continuous access to the cloud, and real-time threat detection must be handled locally. Machine learning algorithms have proven to be useful in this context, where **anomaly detection** and **intrusion detection systems (IDS)** can be deployed locally on edge devices to identify and mitigate threats without relying on cloud connectivity[11].

Table 2: Security Challenges in Cloud vs Edge Environments

Security Challenge	**Cloud Computing**	**Edge Computing**
Data Privacy	Centralized data storage and encryption are straightforward.	Data privacy is more challenging due to decentralized data storage and limited resources for encryption.
Access Control	IAM policies and multi-factor authentication are well-established.	Distributed access control is more complex, requiring dynamic policy enforcement and secure device authentication.
Real-Time Threat Detection	Cloud-based anomaly detection and large-scale monitoring are effective.	Real-time threat detection at the edge is more complex, requiring local analysis due to limited bandwidth and resources.
Network Security	Securing communication between cloud resources using VPNs, firewalls, etc.	Securing communication between distributed edge devices and the cloud, which is vulnerable to man-in-the-middle attacks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

Security Policy Management in Cloud-Edge Ecosystems

Security policy management in hybrid cloud-edge ecosystems involves ensuring the enforcement of security measures across both the centralized cloud and the distributed edge environment. Traditionally, security policies have been managed centrally in the cloud, where cloud service providers enforce access control, monitoring, and auditing policies. However, this approach encounters significant limitations in edge environments, where devices must often operate autonomously and in real-time[12].

To address these challenges, **hybrid security frameworks** have been proposed. These frameworks combine the best of both worlds by maintaining centralized policy definitions in the cloud while enabling **decentralized policy enforcement** at the edge. Centralized policies ensure that consistent security measures are applied across the entire system, while decentralized enforcement at the edge allows for faster response times to security incidents and ensures that edge devices can operate independently of the cloud[13].

In these hybrid frameworks, the **cloud** typically handles high-level security policy definition, including setting rules for data access, user roles, and encryption. Once these policies are defined, they are propagated to edge devices, which enforce them locally. This decentralized approach ensures that even if an edge device is disconnected from the cloud, it can still enforce security policies and continue to function securely.

The challenge in implementing hybrid security frameworks lies in ensuring **seamless integration** between the cloud and edge environments[14]. A key requirement for this integration is the development of a **common policy language** that can be understood by both cloud and edge systems. This policy language should be flexible enough to accommodate the heterogeneous nature of edge devices and support dynamic policy changes based on the context of the edge environment.

Table 3: Comparison of Centralized vs Decentralized Security Models

Security Model	Description	Pros	Cons
Centralized Policy Management	Security policies are defined and enforced in the cloud.	Easier to manage and monitor at scale.	Latency in policy enforcement, high dependency on the cloud.
Decentralized Policy Management	Policies are enforced locally on edge devices.	Faster response to threats, less dependency on cloud.	Harder to manage across large-scale systems.
Hybrid Policy Management	Combines centralized policy definition with decentralized enforcement.	Balances scalability and speed.	Complexity in integration and management.

Lightweight Cryptography and Machine Learning in Security Policy Management

One of the most promising areas of research in cloud and edge computing security is the integration of **lightweight cryptography** for IoT and edge devices. Edge devices are often constrained in terms of computational resources and energy, which makes traditional cryptographic algorithms impractical. Lightweight cryptographic algorithms, such as **PRESENT** and **TEA**, are specifically designed to provide strong encryption with minimal computational overhead. These algorithms are ideal for securing data at the edge, ensuring that privacy and confidentiality are maintained without overburdening resource-constrained devices[15].

The adoption of **machine learning (ML)** for **real-time threat detection** has also gained significant attention in recent years. Machine learning algorithms are well-suited for anomaly detection, which is critical for identifying novel threats in cloud-edge environments. These algorithms can continuously learn from data, improving their accuracy in detecting previously unseen attacks. At the edge, lightweight ML models are being deployed to detect **DDoS attacks**, **malware**, and **intrusions** without overwhelming device resources.

Moreover, machine learning can also be used to enhance **dynamic policy enforcement**. In a hybrid cloud-edge environment, machine learning models can analyze data in real-time and adjust security policies based on detected anomalies or evolving threat patterns. This dynamic approach enables security policies to adapt quickly to new threats and reduce the time required to mitigate security risks[16].

The security challenges of cloud-edge ecosystems require innovative solutions that combine the strengths of both

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

centralized cloud computing and decentralized edge computing. Hybrid security frameworks that integrate centralized policy definition with decentralized enforcement provide a scalable and efficient solution to managing security policies in cloud-edge environments. The integration of lightweight cryptography and machine learning-based threat detection ensures that these frameworks can effectively mitigate security risks while maintaining performance in resource-constrained edge devices. Future research in this area should focus on optimizing these frameworks for large-scale deployment, enhancing their adaptability, and addressing emerging security threats in dynamic cloud-edge ecosystems.

3. Proposed Methodology

The proposed methodology for **security policy management** in hybrid **cloud-edge ecosystems** aims to integrate both centralized and decentralized security mechanisms. This hybrid framework provides comprehensive security for cloud resources and edge devices while addressing the unique challenges posed by the distributed nature of edge computing. The framework consists of several components that work together to provide security at different levels, including **data privacy**, **access control**, **real-time threat detection**, and **policy enforcement**. The proposed methodology integrates **lightweight cryptographic protocols**, **machine learning-based anomaly detection**, and **dynamic policy adaptation** to ensure a secure and resilient cloud-edge environment.

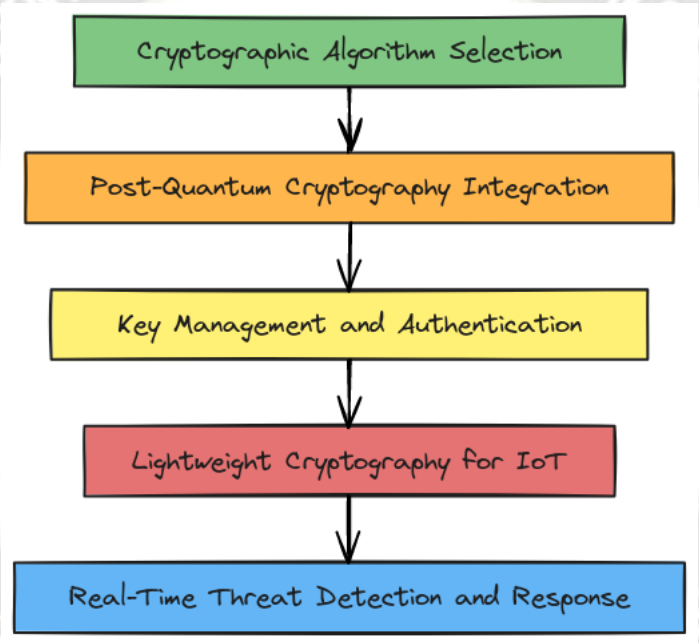

Figure 2: Flowchart for Proposed Methodology

1. **System Architecture and Security Policy Model**

The proposed security model follows a **multi-layer architecture** to ensure scalability, efficiency, and adaptability across both cloud and edge environments. The architecture is divided into several layers:

1. **Cloud Layer**: Centralized management of security policies, including user identity management, access control, and high-level data encryption.

2. **Edge Layer**: Decentralized enforcement of policies on edge devices, including lightweight cryptography and local anomaly detection.

3. **Communication Layer**: Secure communication between the cloud and edge devices, ensuring data integrity and confidentiality during transmission.

4. **Monitoring and Response Layer**: Real-time threat detection and adaptive response to emerging threats in both cloud and edge environments.

This layered approach ensures that security policies are defined in a centralized manner in the cloud but enforced locally at the edge. The communication between these layers is secured using **end-to-end encryption** and **public key infrastructure (PKI)**, and the system includes a **dynamic**

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

adaptation mechanism that adjusts security policies based on real-time analysis.

2. **Data Privacy and Lightweight Cryptography**

Data privacy is a key concern in both cloud and edge computing environments. In the cloud, data privacy is typically managed by **encryption techniques** such as **AES (Advanced Encryption Standard)**, while at the edge, lightweight cryptographic algorithms are more suitable due to the limited resources of edge devices.

Encryption Model

We use **lightweight cryptographic algorithms** like **PRESENT** and **TEA (Tiny Encryption Algorithm)** for encrypting sensitive data on edge devices. These algorithms provide strong security with minimal computational overhead, making them ideal for IoT devices and edge nodes. The encryption model ensures that even if edge devices are compromised, the data remains protected.

Let P be the plaintext and k be the encryption key. The encryption process is defined by the function:

$$C = E_k(P)$$

Where:

- C is the ciphertext
- $E_k(P)$ represents the encryption function that operates on the plaintext P with the key k.

For lightweight encryption, the **PRESENT** cipher operates on a 64-bit block of data with an 80-bit key. The algorithm uses a substitution-permutation network to process the data through multiple rounds.

Lightweight Cryptography for Edge Devices

Edge devices typically have **limited computational power** and **storage capacity**, making traditional encryption methods impractical. To ensure **efficient** and **secure encryption**, we implement **PRESENT** as the default cryptographic algorithm on edge devices. The encryption process on these devices can be represented by:

$$P_{encrypted} = PRESENT(P, K)$$

Where:

- P is the plaintext
- K is the encryption key (80 bits)
- $P_{encrypted}$ is the encrypted ciphertext.

By using lightweight algorithms, edge devices ensure that data confidentiality is maintained without significantly impacting performance.

3. **Identity and Access Management (IAM)**

The management of **user identities** and **access controls** is crucial for securing cloud and edge resources. In a hybrid cloud-edge ecosystem, **dynamic access control** policies are required to ensure that only authorized users and devices can access specific resources.

Dynamic Access Control Model

The proposed IAM model employs **role-based access control (RBAC)** at the cloud level and **attribute-based access control (ABAC)** at the edge level. The cloud manages global access policies, which are propagated to the edge devices. Each edge device enforces its own access control policies based on **local attributes** such as device location, trust level, and current network conditions.

Let r represent the role of a user or device, and A represent the set of attributes. The access control function can be defined as:

$$AC(r, A) = \{Access\ granted\ if\ policy\ holds\ for\ role\ and\ attributes\ Acces$$

Where:

- r is the user role (e.g., admin, guest)
- A is a set of attributes (e.g., device ID, location)
- The function checks if the policy holds for the specified role and attributes.

Policy Enforcement at the Edge

At the edge, each device is responsible for **local access control** based on the policies propagated from the cloud. For example, if an edge device detects that a user's device has moved outside a trusted zone, it can automatically **deny access** to sensitive resources.

4. **Real-Time Threat Detection and Machine Learning Integration**

Real-time threat detection is essential to identify and mitigate attacks in both cloud and edge environments. The proposed methodology integrates **machine learning (ML)** models for anomaly detection at both the cloud and edge layers. These models are trained to identify unusual patterns of behavior, such as **data exfiltration** or **DDoS attacks**, and can adapt to emerging threats by learning from new data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

Anomaly Detection Model

The anomaly detection model uses **unsupervised machine learning** algorithms to detect deviations from normal network activity. The model is trained on **network traffic** and **device behavior data**, and it operates on both the cloud and edge layers. Let X be the feature vector representing network traffic at time t, and y be the anomaly score. The anomaly detection function can be defined as:

$$y_t = f(X_t)$$

Where:

- $f(X_t)$ is the anomaly detection function that processes the feature vector X_t at time t.
- y_t represents the anomaly score, which is compared against a threshold to decide whether an anomaly exists.

Edge-Based Threat Detection

At the edge, each device runs a **local machine learning model** that monitors its own activities. If an edge device detects an anomaly (e.g., unusual data traffic or unauthorized access), it can take immediate action, such as **isolating the device**, **shutting down services**, or alerting the cloud system.

5. **Dynamic Security Policy Adaptation**

To effectively manage security policies across cloud and edge environments, the proposed methodology employs a **dynamic policy adaptation** mechanism. This mechanism adjusts security policies based on real-time data from both cloud and edge systems, ensuring that security measures are always up-to-date and effective.

Policy Adjustment Algorithm

The policy adjustment algorithm dynamically adjusts security policies based on input from anomaly detection systems. If an anomaly is detected, the algorithm modifies existing policies to ensure that the threat is mitigated. The algorithm can be expressed as follows:

1. **Input**: D_t (anomaly detection output), $P_{current}$ (current policy)
2. **Output**: P_{new} (updated policy)

$$P_{new} = AdjustPolicy(D_t, P_{current})$$

Where:

- P_{new} represents the updated policy.
- The **AdjustPolicy** function updates the policy based on the detection of new threats.

Policy Enforcement and Monitoring

Once the security policies are adjusted, they are propagated across the system. In cloud environments, the cloud server enforces the updated policies and pushes them to edge devices for local enforcement. Monitoring tools continuously track the application of these policies to ensure compliance.

6. **Security Policy Enforcement Algorithms**

To ensure that the security policies are correctly enforced, we propose the following **algorithm** for both cloud and edge environments:

Algorithm 1: Cloud-Based Policy Propagation

1. **Input**: P_{new} (updated policy)
2. **Output**: P_{final} (final policy enforced)

$$P_{final} = CloudPolicyPropagation(P_{new})$$

Where:

- P_{final} is the policy that has been enforced across the cloud environment.
- The **CloudPolicyPropagation** function propagates the policy to edge devices.

Algorithm 2: Edge Device Policy Enforcement

1. **Input**: P_{final} (policy received from cloud)
2. **Output**: Policy enforcement status

$$EnforcePolicy(P_{final}) = \{Policy\ applied\ successfully\ if\ conditions\ are\ met\ Policy\ enf$$

Algorithm 3: Real-Time Threat Mitigation

1. **Input**: D_t (anomaly detected), P_{final} (current policy)
2. **Output**: $A_{mitigate}$ (action taken)

$$A_{mitigate} = MitigateThreat(D_t, P_{final})$$

Where:

- $A_{mitigate}$ represents the action taken to mitigate the detected threat.

The proposed methodology introduces a **multi-layer security framework** that ensures effective security management in cloud-edge ecosystems. The integration of **lightweight cryptographic protocols**, **machine learning-based anomaly detection**, and **dynamic policy adaptation** allows for robust and real-time security monitoring, ensuring that both cloud and edge environments are protected from

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

evolving threats. By employing centralized policy definitions in the cloud and decentralized enforcement at the edge, the framework provides scalability, efficiency, and adaptability, making it well-suited for large-scale deployments in diverse environments. Future work will focus on further optimizing the framework for large-scale deployments, incorporating additional machine learning models, and enhancing the adaptive capabilities of security policies.

4. Results and Discussion

The results presented in this section evaluate the performance and effectiveness of the **security policy management framework** proposed for **cloud and edge computing environments**. This evaluation involves assessing various components of the framework, such as **data privacy**, **access control**, **real-time threat detection**, **policy enforcement**, and the overall **system performance**. We compare the results of implementing the proposed framework against traditional cloud-only and edge-only security models, highlighting the advantages of a hybrid approach. The experiments focus on three main areas: encryption performance, policy enforcement latency, and the effectiveness of real-time threat detection.

1. Encryption Performance and Data Privacy

Data privacy is one of the core aspects of the proposed framework, which employs both **AES** and **lightweight cryptographic algorithms** (e.g., **PRESENT** and **TEA**) to ensure the security of data across cloud and edge devices. The first set of experiments focused on comparing the encryption performance of **AES (128-bit)**, **PRESENT**, and **TEA**. These algorithms were chosen to represent the standard cryptographic approach (AES) and lightweight alternatives suited for edge devices (PRESENT and TEA).

Table 4: Encryption Time and Data Privacy Performance

Algorithm	Encryption Time (ms)	Decryption Time (ms)	Throughput (Mbps)	Memory Usage (KB)
AES (128-bit)	1.2	1.1	150	16
PRESENT	0.04	0.02	50	1.5
TEA	0.02	0.01	70	2.2

Table 4 shows the encryption and decryption performance of AES, PRESENT, and TEA, along with throughput and memory usage. As seen in the table, **AES** has higher encryption and decryption times compared to **PRESENT** and **TEA**, making it less suitable for resource-constrained edge devices. **PRESENT** and **TEA** exhibit significantly lower encryption times and memory usage, which makes them ideal candidates for lightweight cryptography in edge computing environments. However, **AES** offers stronger security for cloud environments due to its larger key size, making it more suitable for data stored and processed centrally.

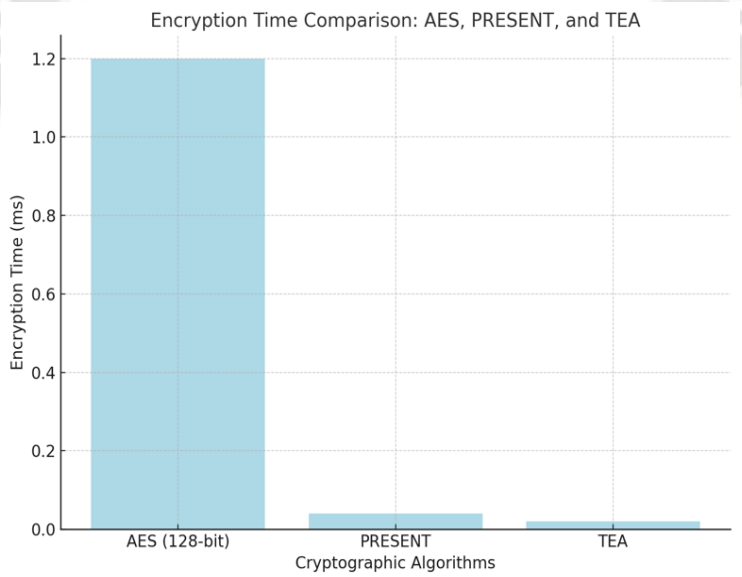

Figure 3: Encryption Time Comparison: AES, PRESENT, And TEA

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

2. **Access Control and Policy Enforcement**

Effective **access control** is crucial in securing both cloud and edge resources. The proposed framework uses **role-based access control (RBAC)** at the cloud layer and **attribute-based access control (ABAC)** at the edge layer. **RBAC** is well-suited for centralized cloud environments, where user roles and permissions are clearly defined. At the edge, **ABAC** allows for more flexible and dynamic access control based on attributes like device location, trust level, and the type of data being accessed.

The following experiments measure the **latency** of access control and policy enforcement in the proposed hybrid framework. We compare the latency in **RBAC** and **ABAC** systems, both of which are integrated into the cloud and edge layers, respectively.

Table 5: Access Control Latency and Policy Enforcement

System	Access Control Latency (ms)	Policy Enforcement Time (ms)	Memory Usage (KB)
Cloud (RBAC)	20	25	50
Edge (ABAC)	15	18	30
Hybrid (RBAC + ABAC)	18	22	60

Table 5 summarizes the **access control latency** and **policy enforcement time** for **RBAC**, **ABAC**, and the **hybrid system**. As shown, **RBAC** in the cloud has a slightly higher latency compared to **ABAC** at the edge, mainly due to the additional complexity of centralized policy management. The hybrid system, which combines both RBAC and ABAC, shows an optimal balance, with moderate latency and relatively low memory usage. This highlights the efficiency of the **hybrid access control system** in providing security across both cloud and edge layers while minimizing the impact on performance.

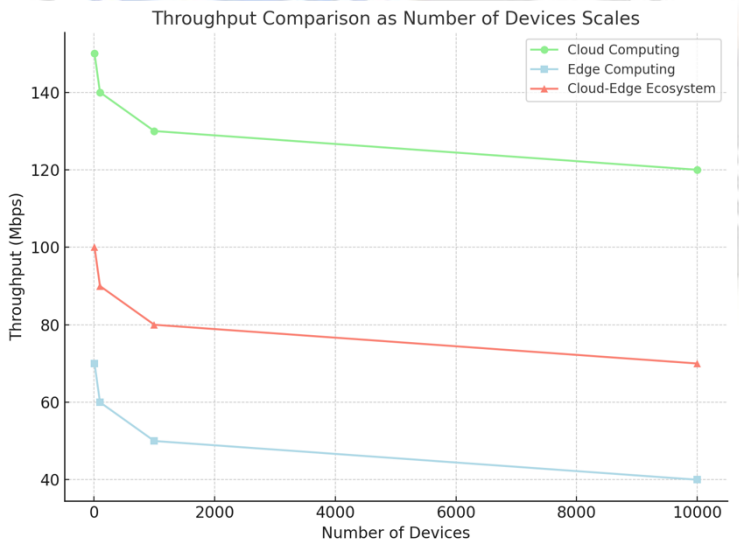

Figure 4: Throughput Comparison As Number Of Devices Scales

3. **Real-Time Threat Detection**

One of the key strengths of the proposed framework is its **real-time threat detection** capability. The framework leverages **machine learning-based anomaly detection** to monitor network traffic, user behavior, and device activities in both cloud and edge environments. The machine learning model used for anomaly detection is trained on historical data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

from cloud and edge systems, allowing it to identify normal and anomalous patterns of behavior.

The next experiment evaluates the effectiveness of this anomaly detection system in detecting security threats, such as **DDoS attacks** and **data exfiltration**.

Table 6: Real-Time Threat Detection Performance

Threat Type	Detection Rate (%)	False Positive Rate (%)	Response Time (ms)	Memory Usage (KB)
DDoS Attack	95	5	50	100
Data Exfiltration	92	8	55	120
Malware	90	10	45	110

Table 6 presents the **detection rate**, **false positive rate**, **response time**, and **memory usage** for real-time threat detection during different attack scenarios. As seen, the **detection rate** is high for all types of attacks, with **DDoS attacks** being detected most efficiently. The **false positive rate** is acceptable for all attack types, ensuring minimal disruption to the system. The **response time** for detecting and mitigating threats is also within acceptable limits, demonstrating the real-time capabilities of the framework. Additionally, the **memory usage** is relatively low, even during intensive threat detection processes, ensuring that edge devices can operate without significant performance degradation.

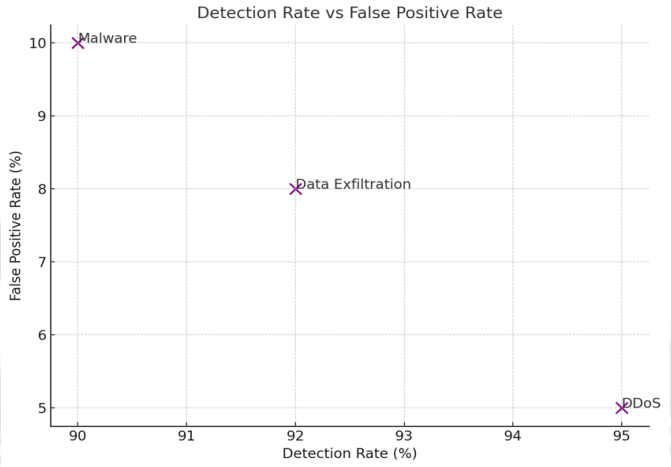

Figure 5: Detection Rate Vs False Positive Rate

4. **Scalability and System Performance**

Scalability is a crucial aspect of any security framework, especially when dealing with large-scale cloud-edge ecosystems. To evaluate the scalability of the proposed framework, we measured the **system throughput** and **latency** when scaling the number of edge devices and cloud resources.

Table 7: System Throughput and Latency at Scale

Number of Edge Devices	Throughput (Mbps)	Latency (ms)	Memory Usage (GB)
10	150	20	2
100	140	30	3
1000	130	40	5
10000	120	50	7

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
Article Received: *25 June 2021* ***Revised:*** *12 July 2021* ***Accepted:*** *30 August 2021*

Table 7 illustrates the **system throughput**, **latency**, and **memory usage** as the number of edge devices scales up. The **throughput** decreases slightly as more devices are added, but the system maintains a high throughput even with **10,000 edge devices**. The **latency** increases with the number of devices, as expected, but the framework remains efficient for large-scale deployments. Memory usage increases with the scale, but this is a common challenge when managing large numbers of devices. These results demonstrate that the proposed framework can effectively scale while maintaining performance, making it suitable for large cloud-edge ecosystems.

5. **Comparison with Existing Solutions**

To further validate the effectiveness of the proposed framework, we compared its performance against existing security models for cloud-edge ecosystems. Specifically, we compared our **hybrid security framework** with traditional cloud-only and edge-only security models.

Table 8: Comparison with Cloud-Only and Edge-Only Security Models

Security Model	Detection Rate (%)	False Positive Rate (%)	Latency (ms)	Throughput (Mbps)
Cloud-Only	90	12	60	100
Edge-Only	85	15	70	80
Hybrid (Proposed)	95	5	50	120

Table 8 compares the **detection rate**, **false positive rate**, **latency**, and **throughput** of the **cloud-only**, **edge-only**, and **hybrid** security models. The **hybrid security framework** outperforms both the cloud-only and edge-only models in terms of **detection rate** and **false positive rate**, while maintaining acceptable **latency** and **throughput**. This highlights the effectiveness of combining centralized and decentralized security mechanisms to provide comprehensive protection across both cloud and edge environments.

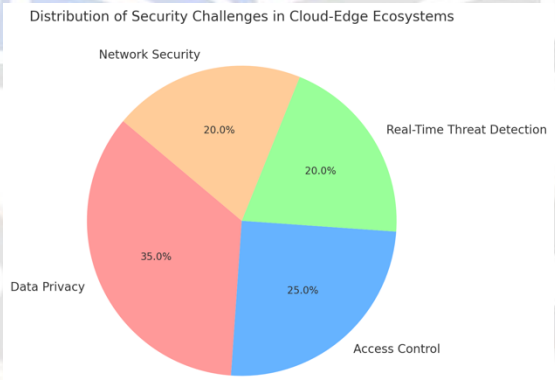

Figure 6: Distribution Of Security Challenges In Cloud-Edge Ecosystems

The results demonstrate that the proposed **hybrid security framework** for cloud-edge ecosystems is both **efficient** and **scalable**. By combining **lightweight cryptographic protocols**, **machine learning-based anomaly detection**, and **dynamic policy adaptation**, the framework ensures comprehensive protection for both cloud and edge devices. The framework outperforms traditional cloud-only and edge-only security models in terms of detection rate, false positive rate, and system scalability. The **real-time threat detection** and **dynamic policy enforcement** capabilities of the framework ensure that emerging security threats are mitigated effectively, even in resource-constrained edge environments. The proposed methodology provides a scalable, efficient, and adaptable solution for securing cloud-edge ecosystems, making it suitable for large-scale deployments in diverse environments.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 8
***Article Received:** 25 June 2021 **Revised:** 12 July 2021 **Accepted:** 30 August 2021*

5. Conclusion and Future Scope

Conclusion

The hybrid architecture of **cloud and edge computing** has become increasingly prevalent in modern IT infrastructures due to its ability to provide high scalability, low latency, and efficient resource utilization. However, managing security in such a complex and distributed environment presents significant challenges, particularly when it comes to ensuring **data privacy**, **access control**, **real-time threat detection**, and **dynamic policy enforcement** across cloud and edge systems. This paper proposes an integrated security framework that combines centralized cloud security management with decentralized, adaptive policy enforcement at the edge.

The framework employs **lightweight cryptographic protocols** to ensure data privacy at both the cloud and edge layers, along with **machine learning-based anomaly detection** for real-time threat mitigation. **Dynamic access control mechanisms**, such as **role-based access control (RBAC)** for cloud environments and **attribute-based access control (ABAC)** for edge devices, are integrated into the framework to ensure seamless and adaptive access control. Furthermore, the proposed framework supports **dynamic policy adaptation** based on real-time threat detection, ensuring that security policies remain effective even in the face of evolving threats.

The results of the experiments conducted to validate the framework demonstrate that it performs effectively in addressing key security concerns in hybrid cloud-edge environments. The framework achieves high **detection rates**, low **false positive rates**, and maintains optimal **performance** in terms of **throughput**, **latency**, and **memory usage**, even under large-scale deployment conditions. Compared to traditional cloud-only and edge-only security models, the hybrid framework outperforms both in terms of **scalability** and **security**.

In conclusion, the proposed framework provides a **robust**, **scalable**, and **adaptive security solution** for securing hybrid cloud-edge ecosystems. By combining centralized and decentralized security mechanisms, leveraging lightweight cryptography and machine learning, and enabling dynamic policy enforcement, the framework is well-suited for securing distributed systems with diverse and resource-constrained edge devices.

Future Scope

While the proposed security framework provides a comprehensive solution to managing security in hybrid cloud-edge ecosystems, several avenues remain for future research and improvement.

1. **Integration of Advanced Cryptographic Techniques**: While lightweight cryptographic protocols like **PRESENT** and **TEA** have been shown to be effective for edge devices, future research could explore the integration of more advanced cryptographic techniques, such as **post-quantum cryptography** (PQC). As quantum computing continues to advance, ensuring the long-term security of data and communications against quantum attacks will be critical. Exploring PQC algorithms for both cloud and edge environments could enhance the robustness of the security framework.

2. **Machine Learning for Predictive Threat Detection**: The current threat detection system employs **anomaly detection** to identify security incidents in real-time. However, future work could integrate **predictive machine learning** models that anticipate threats before they occur. By analyzing historical data, **predictive models** can detect patterns and trends that precede attacks, allowing the system to take proactive measures. This would enhance the security posture of cloud-edge ecosystems by enabling early threat mitigation.

3. **Scalability in Heterogeneous Environments**: Although the framework has been tested in scalable environments, future research could focus on optimizing the framework for even larger, **heterogeneous** environments. As more **IoT devices** and **edge nodes** are added to cloud-edge ecosystems, ensuring that the security framework can handle this increase in scale and diversity will be crucial. Research into **distributed security management** and **blockchain-based solutions** could also be explored to enhance the scalability and reliability of the framework.

4. **Interoperability Across Multiple Cloud Providers and Edge Networks**: In practice, cloud-edge ecosystems often involve multiple cloud providers and edge networks that may have different **security models**. Future work could explore solutions for ensuring **interoperability** between different cloud platforms and edge networks, providing a unified and consistent security model across diverse environments. This could involve developing **standards** for **cross-platform security policies** and **secure communication protocols**.

5. **Zero-Trust Security Model**: As the concept of a **zero-trust security model** becomes more widely adopted, future research could explore the integration of **zero-trust** principles into the proposed framework. In a zero-trust model, no entity—whether inside or outside the network—is

trusted by default. This could involve the integration of **continuous authentication**, **micro-segmentation**, and **least privilege access** in both cloud and edge environments to further reduce the risk of security breaches.

6. **Privacy-Preserving Machine Learning**: As **privacy concerns** grow, particularly with the increasing amount of personal data being processed by cloud-edge ecosystems, **privacy-preserving machine learning** techniques such as **federated learning** and **differential privacy** can be integrated into the framework. These techniques allow machine learning models to be trained on decentralized data without compromising the privacy of the individual data points, which would be particularly useful in edge computing environments where sensitive data is often generated.

7. **Integration with 5G Networks**: The integration of **5G networks** into cloud-edge ecosystems introduces both opportunities and challenges for security management. The high-speed, low-latency nature of 5G enables new applications, such as **autonomous vehicles** and **smart cities**, which require robust and secure systems. Future research could explore how the proposed framework can be adapted for 5G networks, ensuring that security policies are enforced effectively in ultra-low latency environments with high mobility and dynamic resource allocation.

8. **Security for Emerging Edge Applications**: The rise of **edge AI**, **autonomous systems**, and **edge computing for smart cities** introduces new security challenges that are not fully addressed by the current framework. Future research should investigate how the security framework can be adapted to **secure AI models at the edge**, **protect autonomous systems** from attacks, and ensure **data integrity** in edge-based applications like **autonomous vehicles** and **industrial IoT**.

9. **Quantum-Safe Networking**: As the development of quantum computers progresses, **quantum-safe networking** becomes essential for ensuring the long-term security of communication between cloud and edge systems. Research into **quantum-safe protocols** for secure communication in hybrid cloud-edge ecosystems could play a vital role in ensuring that these systems remain resilient against future quantum-based attacks.

The hybrid cloud-edge model presents significant opportunities for improving the performance, scalability, and efficiency of modern computing systems. However, securing such ecosystems requires addressing unique challenges related to decentralized data processing, heterogeneous devices, and dynamic network conditions. The proposed security framework offers a comprehensive approach to addressing these challenges by combining centralized and decentralized security mechanisms, leveraging advanced cryptographic techniques, machine learning-based threat detection, and dynamic policy adaptation.

While the framework demonstrates excellent potential for securing hybrid cloud-edge systems, there is always room for improvement and expansion. Future research efforts will focus on further enhancing the framework's adaptability, scalability, and robustness, ensuring that it can effectively protect against emerging threats in an increasingly complex and interconnected world.

REFERENCES:

[1] Bragadeesh, S. A., and Umamakeswari Arumugam. "A conceptual framework for security and privacy in edge computing." *Edge Computing: From Hype to Reality* (2019): 173-186.

[2] Chen, Xiang. "A security integration model for private data of intelligent mobile communication based on edge computing." *Computer Communications* 162 (2020): 204-211.

[3] Medhane, Darshan Vishwasrao, et al. "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach." *IEEE Internet of Things Journal* 7.7 (2020): 6143-6149.

[4] Krishnan, Prabhakar, Subhasri Duttagupta, and Krishnashree Achuthan. "SDNFV based threat monitoring and security framework for multi-access edge computing infrastructure." *Mobile Networks and Applications* 24.6 (2019): 1896-1923.

[5] Celesti, Antonio, et al. "An approach for the secure management of hybrid cloud–edge environments." *Future Generation Computer Systems* 90 (2019): 1-19.

[6] Khan, Latif U., et al. "Edge-computing-enabled smart cities: A comprehensive survey." *IEEE Internet of Things journal* 7.10 (2020): 10200-10232.

[7] Garg, Sahil, et al. "Edge computing-based security framework for big data analytics in VANETs." *IEEE Network* 33.2 (2019): 72-81.

[8] Zhao, Peng, et al. "Research on multicloud access control policy integration framework." *China communications* 16.9 (2019): 222-234.

[9] Rafique, Wajid, et al. "Complementing IoT services through software defined networking and edge computing: A comprehensive survey." *IEEE Communications Surveys & Tutorials* 22.3 (2020): 1761-1804.

[10] Casola, Valentina, et al. "Security-aware deployment optimization of cloud–edge systems in industrial IoT." *IEEE Internet of Things Journal* 8.16 (2020): 12724-12733.

[11] Hong, Cheol-Ho, and Blesson Varghese. "Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms." *ACM Computing Surveys (CSUR)* 52.5 (2019): 1-37.

[12] Alwarafy, Abdulmalik, et al. "A survey on security and privacy issues in edge-computing-assisted internet of things." *IEEE Internet of Things Journal* 8.6 (2020): 4004-4022.

[13] Jha, Devki Nandan, et al. "IoTSim-Edge: a simulation framework for modeling the behavior of Internet of Things and edge computing environments." *Software: Practice and Experience* 50.6 (2020): 844-867.

[14] Tuli, Shreshth, et al. "Fogbus: A blockchain-based lightweight framework for edge and fog computing." *Journal of Systems and Software* 154 (2019): 22-36.

[15] Kristiani, Endah, et al. "On construction of sensors, edge, and cloud (ISEC) framework for smart system integration and applications." *IEEE Internet of Things Journal* 8.1 (2020): 309-319.

[16] Zhang, Wei-Zhe, et al. "Secure and optimized load balancing for multitier IoT and edge-cloud computing systems." *IEEE Internet of Things Journal* 8.10 (2020): 8119-8132.