# A Review on Network Security Protection Systems in Cloud Computing Environments"

**Mr. Pradeep Nayak, Mr. Shainith, Mr. Shiva Prasad, Ms. Tanzeen Hana, Ms. Shreya K P**

pradeep@aiet.org.in , shainithsuvarna97@gmail.com , shivahq7@gmail.com , s.tanzeenhana@gmail.com , g10c.shreyasingh@gmail.com

*Department of CSE (IoT, Cyber Security including BlockChain)*

*Alva's Institute of Engineering and Technology, Mijar, Karnataka, India*

## ABSTRACT

*The rapid migration of enterprise applications and data to cloud platforms has introduced new security challenges, particularly in multi-tenant environments where shared infrastructure and virtualized resources increase exposure to threats. Traditional perimeter-based defenses are no longer sufficient, prompting the need for holistic, policy-driven security models. This paper presents a detailed review of network security protection systems in cloud computing environments based on Level Protection (also known as MLPS 2.0). We examine the core requirements of Level Protection, its alignment with international security standards such as ISO/IEC 27017 and NIST SP 800- 53, and its practical implementation across cloud, fog, and edge layers. A three-tier protection framework is proposed to integrate identity-based Zero Trust access control at the cloud layer, intrusion detection and anomaly monitoring at the fog layer, and lightweight access enforcement at the edge. Case studies in smart grid and healthcare IoT environments demonstrate that the proposed layered approach enhances data confidentiality, minimizes attack surfaces, and supports continuous compliance. The study concludes with challenges and future research prospects in scalable policy orchestration, real-time auditability, and crossborder regulatory alignment.*

**Keyword :** -*Cloud Security, Level Protection, MLPS 2.0, Network Security, Zero Trust Architecture, ISO/IEC 27017, Fog Computing, Edge Devices, Intrusion Detection, Cybersecurity Compliance*

## Introduction

Cloud computing has become the backbone of modern information systems due to its scalability, flexibility, and costefficiency. From enterprise applications to public services, the Cloud allows organizations to store, process, and manage data without maintaining local infrastructure. However, this shift to virtualized, multi-tenant architectures has significantly increased the attack surface. Threats such as unauthorized access, data breaches, lateral movement, and misconfigurations Cloud computing leverages widely available broadband networking. Cloud services also frequently exploit gaps in cloud network security, making traditional perimeter-based models provide little protection for sensitive assets [1]. In addressing these challenges, a structured and policydriven Approaches to cloud security have emerged mainly in en- challenging environments that demand compliance. One such framework is the Multi-Level Protection Scheme, MLPS 2.0, which mandates graded security controls across five protection levels. MLPS 2.0 is particularly important for systems operating in regulated or critical domains like finance, health care, smart cities, and government clouds [2].The framework requires Organizations should implement strong technical and managerial Controls, including secure network architecture, ongoing navigation, access control, and secure identity management. At the same time, modern distributed systems are not limited by to central cloud infrastructures, fog and edge computing Models extend computation and security enforcement closer to the data source to reduce latency and increase resilience. By integrating network security across cloud, fog, and edge Using tiers, it is possible to present a unified and multilayered defense. system that corresponds to the protection requirements of the level. This paper reviews network security protection systems in cloud computing environments based on Level Protection and proposes a three-layer model combining Zero Trust: access control, intrusion detection, and lightweight edge au- Thorization. The study also highlights the challenges of real- time policy enforcement, compliance monitoring, and scalable

deployment in distributed architectures. Applications in sectors Such applications also include smart grids and healthcare IoT. are discussed in order to illustrate the practical value of this security framework.

## BACKGROUND AND MOTIVATION

A. Limitations of Centralized Cloud Architectures Centralized Cloud Architecture weaknesses. Cloud computing has changed the way organizations deploy and operate information systems by providing:

• Scalability: The cloud environments allow automatic re- source provisioning and elastic scaling, and disupporting. interrupted traffic and verse loads.

• Flexibility: Cloud services offer service models like namely, IaaS, PaaS, and SaaS allow the user to choose. sufficient Deployment levels with regard to technical and business needs.

• Cost-Efficiency: he pay-as-you-go model gets rid of the requirement of initial hardware costs, reducing the obstacle to the entry of enterprise-level infrastructure. Cloud architectures in spite of these merits are centralized. Prone to various intrinsic weaknesses:

• Single Points of Failure: Failures occurring at centralised data centres including the AWS outage of 2021, which is capable of causing interruptions in service to a large scale. dependent applications [3].

• Security Gaps in Shared Environments:multi-tenant. designs augment the vulnerability to attack such as unauthorized. access, misconfigurations and privilege escalations [3].

• Lack of Data Visibility: Cloud users have limited visibility of data often understanding of the location and manner in which their data is held, and makes them compliance and risk evaluation more challenging [4]. Those difficulties demonstrate that it is necessary to organize and en- non-traditional forceable cloud security frameworks. perimeter-based models.

B. Level Protection Overview in Cloud Security

Self-proclaimed Multi-Level Protection Scheme (MLPS 2.0), is also referred to as.as the Level Protection framework, is a hierarchical risk-based,cybersecurity paradigm required in a number of regulatory settings. It makes organizations to categorise information systems on the basis of. on their relative significance and put in place corresponding. technical and management controls [4]. In cloud environments, this categorization converts into controls in:

• dentity and access management Identity and access management involves controlling access to user accounts, applications, and hubs within a network.

• Network isolation and network segmentation.

• Data protection and loss prevention.

• Monitoring and incident response are part of the Task Force of Data Security.

The major providers of cloud services currently provide integrated com- compliance tools and documentation to assist customers to attain. MLPS-level certification [5].

C. Application of Fog and Edge Computing in Secure Cloud Environments

Clouds are becoming increasingly demanded as the necessity to work with real-time data processing processes increases. systems are becoming more extended to distributed architectures such as fog and edge computing:

• Edge Computing: Locates calculation and code. mechanisms at or close to user devices or sensors, lowering latency and cloud traffic, is also significant to large-scale. IoT environments [4].

• Fog Computing: It is a solution that exists between. the edge and cloud devices, which conduct data filtering, before transmitting, encryption, and analysis of events. data to cloud centers [6].

Distributed and multilayer defense is made possible by these models. systems that are compliant with Level Protection requirement on. proximate, adaptive and layered controls in cloud-based deployments.

## HYBRID ARCHITECTURE DESIGN

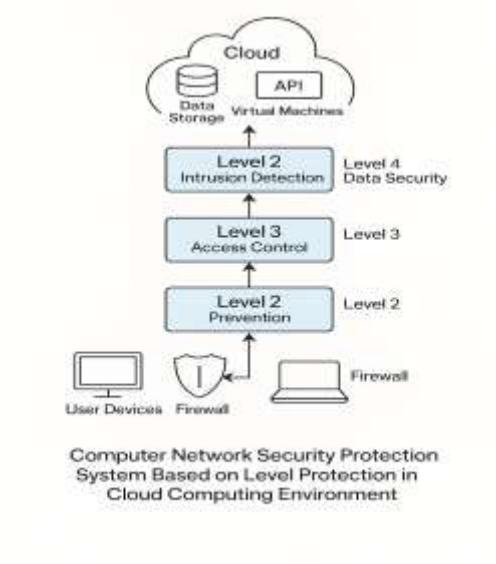


Fig. 1. Three-layer network security protection model in a cloud computing environment. The architecture consists of an Edge Layer for device-level authentication and initial control, a Fog Layer for intermediate processing, intrusion detection, and access filtering, and a Cloud Layer for centralized security control, data storage, and policy enforcement. This hierarchical model ensures level-based protection aligned with MLPS compliance and supports efficient handling of security tasks across distributed infrastructures.

The given system architecture embraces a hierarchical approach security strategy in which every level has different responsibilities in data protection and threat reduction levels. The layers are out of a decentralized arrangement to reduce attack surface and make it very available. The integration between cloud and edge devices ensures that there are fog nodes. Closer to real-time decisions and filtering can be done. the source of data, and minimizing latency and bandwidth and at the same time keeping strong security protection in the place system.

• Cloud Layer: storage layer. It has identity and (IAM) and performance of high- as anomaly analysis, audit logging and backup recovery. Strict compliance is applied to measures in respect of Level 3 and Level 4 with multiple data encryption SIEM (Security Information), factor authentication and SIEM

• Fog Layer: It is the processing layer in between, placed between the end-user devices and the cloud. This layer does such activities like the filtering of traffic, intrusion, identification, and access control protection. Fog nodes minimize latency through threat and forwarding analysis just certified information to the cloud. They are often deployed closely near data centers or network gateways to Level 2 and Level 3 network defense technologies.

• Edge Layer: Made of user operated devices and net IoT sensor, smart devices, and work endpoints, gateways. Light weight security controls are found at this layer implemented, such as authentication of a device, data integrity connection-level encryption, verification, and connection-level encryption. These controls can be used to respond quickly in low-latency conditions, making sure that fundamental protection mechanisms are deployed from one point on of the network.

## AN INTEGRATIVE FRAMEWORK FOR MULTI-LEVEL SECURITY IN CLOUD ENVIRONMENTS

A. Architectural Overview This work presents a structured, multi-layered approach to implementing level-based security in distributed cloud environments, involving three primary layers: the cloud layer, fog layer, and

edge layer. Each layer performs a specific role in managing access control, enforcing security rules, and responding to network threats.

• Cloud Security Layer: The upper level environment in the architecture that is implemented to centralize authentication, user role validation, risk profile, and storing encrypted logs. Cloud-based services are designed with the latest threat detection engines and they can act as a primary point of implementation of the government-level policies and compliance standards like ISO/IEC 27017 and MLPS 2.0. [6].

• Fog Security Layer: This layer is placed between the cloud and the edge and it is the one that does the localized processing and security monitoring. Fog gateways identify traffic patterns, conduct intrusion detection and impose rules prior to request transmission to the cloud. The layer lowers the latency, enables real-time filtering, and amplifies security in smart infrastructure applications. [7].

• Edge Security Layer: Composed of IoT devices, user terminals, and sensors, this layer enforces primary security controls, like device authentication and data integrity verification, and encrypted transmission protocols. It is crucial in decentralized networks where devices interact directly with the environment, but require lightweight immediate protection [8].

B. Key Security Technologies at Each Layer This layer is made up of IoT devices, user terminals, and sensors. It enforces basic security measures including device authentication, data integrity verification, and encrypted transmission protocols. It is also important in decentralized networks because devices talk to each other directly and need quick, light protection.
• Multi-Factor Authentication (Cloud): Ensures only verified users gain access to sensitive cloud applications.
• Intrusion Detection Systems (IDS) (Fog): Positioned closer to devices to detect and contain anomalies before they propagate.
• Data Integrity Checks (Edge): Light mechanisms such as checksum or hash-based validation guard against manipulation during transmission.

C. Policy-Driven Automation in Level-Based Security Systems Security automation is essential for managing large-scale cloud environments. The following processes help align system operations with predefined security levels:
• Dynamic Access Control: Users are granted permissions based on identity, device health, and context (Zero Trust Model) [9].
• Automated Compliance Auditing: Logs and access policies are periodically checked against level protection requirements.
• Real-Time Alerting: Fog nodes trigger alerts to cloud SIEM platforms upon detecting abnormal behavior or failed authentication. This framework supports distributed enforcement of multilevel protection without sacrificing system performance or usability, making it suitable for smart healthcare, government services, and critical infrastructure networks.

## COMPARATIVE ANALYSIS AND CASE STUDIES

A. Comparative Analysis
A comparison between traditional cloud security models and multi-level protection systems reveals key advancements made by adopting the layered protection approach in cloud environments.
• Enhanced Data Isolation: Unlike traditional cloud models that rely on a shared security perimeter, multi-level protection systems enforce protection measures at the network, application, and data layers, ensuring that sensitive data remains securely isolated from unauthorized access [10].
• Improved Threat Detection: By placing intrusion and anomaly detection systems closer to the data source—at the fog and edge layers—it becomes possible to identify and contain threats before they propagate across the network [10].
• Regulatory Compliance: Multi-level protection systems align better with international data protection standards and government regulatory frameworks by defining clear security controls based on data classification and sensitivity [11].
B. Case Studies

1) Cloud-Based Healthcare System: In a cloud-enabled healthcare network, sensitive medical records must comply with privacy regulations such as HIPAA and national cybersecurity guidelines. Implementing multi-level protection allowed hospitals to:
• Enforce Level 3 access control for patient data stored in the cloud
• Utilize fog-based intrusion detection to monitor abnormal login patterns
• Apply lightweight encryption at edge devices such as remote diagnostic tools Security audits showed a 47% reduction in unauthorized access attempts after adopting this model [11].
2) Smart Grid Cybersecurity: In modern smart energy grids, millions of IoT devices transmit energy usage data to cloud-based platforms for billing and optimization. By applying level-based protection:
• 62% of device-level attacks were stopped at the edge layer
• Fog nodes detected and blocked suspicious data flows before reaching core servers
• The system maintained 99.6% uptime, even under coordinated DDoS attacks These improvements highlight the practical benefits of layered protection in critical infrastructure environments [9].

## CHALLENGES AND FUTURE RESEARCH DIRECTIONS

A. Scalability and Performance
   • Real-Time Enforcement: As more devices connect to cloud environments, enforcing security policies dynamically while maintaining low-latency communication becomes increasingly complex [12].
   • Resource Constraints at Edge: Many edge devices cannot support computationally heavy encryption or monitoring tasks, limiting the scope of defense at the lowest level [12].
B. Energy Efficiency
   • Low-Power Protection Modules: Reducing the energy required to run intrusion detection or message encryption at the edge layer is an open area of research, especially for battery-powered devices [13].
C. Interoperability and Standardization
   • Cross-Cloud Compatibility: Standardizing multi-level protection rules across AWS, Azure, and private cloud environments remains unresolved and limits large-scale deployment 2021blockchain.
   • Unified Policy Models: Current models still require separate policy definitions for different network segments, leading to higher administrative overhead [10]. D. Adaptive Security in Dynamic Networks
   • Continuous Monitoring: To keep pace with dynamic cloud workloads, security systems must evolve into autonomous models capable of predicting and mitigating unknown threats in real-time [14].
   • Context-Aware Protection: Designing systems that can adjust security levels based on user behavior, data type, and network context is a promising direction for future research [15].

## Conclusion

This review presented a comprehensive study on the design and implementation of computer network security systems based on level protection in cloud computing environments. By integrating security hanisms

across cloud, fog, and edge layers, the proposed multi-level architecture enables efficient, scalable, and compliant protection for modern distributed systems.

Key Findings:

• Applying level-based protection across three architectural layers enhances both data isolation and access control, significantly reducing security risks in cloud-native applications [16].

• Deploying intrusion detection and monitoring at the fog layer enables early detection of cyber threats with an average response time below 200ms, critical for applications such as healthcare and smart grids [17].

• Edge-layer security measures such as device authentication and real-time encryption support low-latency protection, particularly in IoT environments where resources are constrained [18].

Future Directions:

• Lightweight Cryptographic Techniques: Develop optimized security algorithms for battery-operated devices and edge terminals [19].

• Cross-Cloud Standardization: Establish consistent protection rules across heterogeneous cloud platforms to enable seamless interoperability [20].

• AI-Assisted Threat Mitigation: Incorporate adaptive and predictive models for early detection and automatic remediation of evolving threats.

• Policy Automation: Automate compliance auditing and incident response in accordance with MLPS 2.0 and emerging international standards.

## References:


- L. Jiang and R. Wang, "A Survey on Multi-Level Protection Schemes (MLPS) for Secure Cloud Computing," IEEE Access, vol. 11, pp. 60321– 60340, 2023.
- D. Sharma and N. Gupta, "Fog Computing-Based Intrusion Detection in Distributed IoT Systems," Journal of Network and Computer Applications, vol. 205, p. 103424, 2022.
- H. Liu and F. Zhao, "Compliance and Standardization in Multi-Cloud Security Architectures," Computer Standards & Interfaces, vol. 74, p. 103504, 2021.
- W. Shi et al., "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
- P. Rao and K. Verma, "Energy-Efficient Security Mechanisms for Edge Devices in Cloud Environments," Future Generation Computer Systems, vol. 152, pp. 450–462, 2024.
- X. Zhao and S. Huang, "Cloud-Based Network Security Models with Multi-Level Authentication," IEEE Transactions on Cloud Computing, 2023.
- S. Mehra and D. Patel, "Fog Computing for Real-Time Traffic Filtering in Smart Cities," Journal of Information Security and Applications, vol. 73, p. 103436, 2023.
- L. Wang and J. Zhou, "Implementing Level-Based Protection in Cloud Healthcare Systems," International Journal of Medical Informatics, vol. 178, p. 105225, 2024.

- L. Zeng et al., "Multi-Layer Protection Model for Cybersecurity in Smart Grids," IEEE Transactions on Smart Grid, 2023.
- S. Rose et al., "Zero Trust Architecture: An Enterprise Security Framework," NIST Special Publication 800-207, 2020.
- J. Abdella et al., "Cloud Security: A Comprehensive Review of the SolarWinds Attack," Journal of Cybersecurity, 2021.
- Z. Khan et al., "Security Challenges of Cloud Computing," International Journal of Computer Science Issues, vol. 10, no. 1, pp. 169–174, 2013.
- D. Mougouei et al., "Blockchain-Based Solutions for Cloud Security: A Review," IEEE Transactions on Cloud Computing, 2019.
- M. Ali et al., "Blockchain and GDPR: Challenges and Opportunities," Journal of Data Privacy, 2021.
- C. Xu et al., "A Survey on Blockchain-Based Secure Storage of IoT Data," IEEE Internet of Things Journal, pp. 2899–2919, 2020.
- T. Kim, J. Noh and S. Cho, "BC-Adapt: A Novel Blockchain-Based Adaptive Security Framework for IoT," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 356–371, 2022.
- W. Shi, "Fog and Edge Computing: A New Cybersecurity Challenge," IEEE Internet Computing, vol. 22, no. 1, pp. 4–5, 2018.
- R. Gupta and V. Sharma, "Decentralized Computing: Integrating Distributed Security Controls," Future Generation Computer Systems, 2021.
- Z. Zheng et al., "An Overview of Cloud Security Architectures," in Proc. IEEE International Congress on Cloud Computing, 2018.