iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80831

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Cyber Security Challenges in Cloud Computing: A Systematic Literature Review and Security Framework

Foram Ajit Chothani[1], Parth Awasthi[2], Dhruv Bhanushali[3], Jeet Bhanushali[4], Sahil Aher[5], Dhruv Goswami[6], Saifuddin Khan[7], Asha Durafe[8]
Department of Electronics and Computer Science Shah and Anchor Kuttchi Engineering College, Chembur, Mumbai, India

Abstract: ***Cloud computing has transformed the modern dig- ital infrastructure by providing scalable and flexible computing resources through the internet. However, the rapid adoption of cloud platforms has introduced several cybersecurity challenges including data breaches, insecure APIs, insider threats, and distributed denial-of-service attacks.***
This paper presents a systematic literature review of cybersecurity challenges in cloud computing by analyzing fifteen research papers published between 2011 and 2025. The study identifies key security vulnerabilities and evaluates existing solutions such as encryption, intrusion detection systems, and access control mechanisms.
Based on the identified research gaps, a cloud security frame- work integrating multi-factor authentication, encryption, and AI-based intrusion detection is proposed to enhance cloud security.
Index Terms: Cloud Computing, Cybersecurity, Cloud Security, Intrusion Detection System, Data Protection.

I. INTRODUCTION

Cloud computing enables organizations to store, process, and manage large volumes of data through remote servers rather than local infrastructure. Service models such as Soft- ware as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) provide flexible computing resources on demand.

Despite its advantages, cloud computing introduces multiple cybersecurity risks due to shared infrastructure, remotedata storage, and multi-tenant environments. Cyber attackers frequently target cloud systems to exploit vulnerabilities such as insecure APIs, misconfigured storage systems, and weak authentication mechanisms.

Ensuring secure cloud environments has therefore become a critical research area. Researchers have proposed various techniques including data encryption, intrusion detection sys- tems, and access control frameworks to mitigate cyber threats. However, existing approaches often lack scalability and real- time threat detection capabilities.

This paper reviews existing research related to cybersecurity challenges in cloud computing and proposes a security framework to improve cloud protection. The rapid adoption of cloud computing has been driven by the increasing demand for scalable infrastructure and cost-efficient resource management. Organizations across sectors such as healthcare, finance, and education are migrating critical workloads to cloud platforms. However, this transition has significantly expanded the attack surface, making cloud environments a primary target for cyber threats.

Unlike traditional systems, cloud environments operate on shared infrastructure and dynamic resource allocation, which introduce unique security challenges. The lack of direct control over physical infrastructure, combined with remote access capabilities, creates new vulnerabilities that are not adequately addressed by conventional security models.

Another critical concern is the complexity of managing security across multiple cloud service models and providers. In multi-cloud and hybrid environments, inconsistent security policies and configurations can lead to gaps that attackers can exploit. Misconfigurations, in particular, have emerged as one of the leading causes of cloud security incidents.

Furthermore, modern cyberattacks are increasingly sophisticated, often involving multi-stage attack strategies that bypass single-layer defenses. This highlights the need for integrated and adaptive security mechanisms rather than isolated solutions.

These challenges indicate that existing approaches are in- sufficient to provide comprehensive protection in cloud environments. Therefore, there is a need for a unified security framework that combines strong access control, data protection, and intelligent threat detection mechanisms.

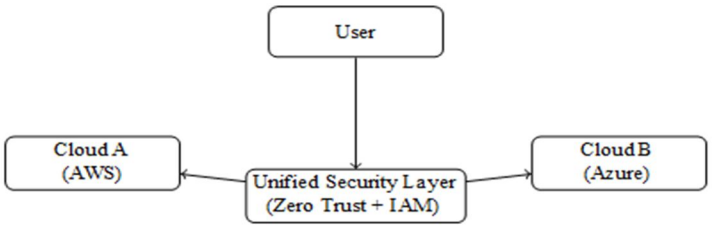


Fig. 1. Multi-Cloud Security Model with Unified Control Layer

II. CYBERSECURITY CHALLENGES IN CLOUD COMPUTING

Cloud computing environments face several security chal- lenges due to their distributed architecture.

A. Data Breaches

Data breaches occur when unauthorized users gain access to sensitive information stored in cloud servers. Weak authen- tication mechanisms and misconfigured storage systems are major causes of such breaches.

B. Insecure APIs

Cloud services depend heavily on APIs to enable commu- nication between users and cloud platforms. Poorly secured APIs may expose cloud systems to cyber attacks.

C. Account Hijacking

Attackers often obtain user credentials through phishing attacks or malware. Once access is gained, attackers can manipulate cloud resources and steal sensitive data.

D. Distributed Denial of Service Attacks

DDoS attacks attempt to overwhelm cloud servers with large volumes of traffic, making services unavailable to legitimate users.

E. E. Insider Threats

Employees or authorized users may misuse their access privileges, which can lead to data leaks or unauthorized modifications.

III. LITERATURE REVIEW

Several researchers have studied security challenges in cloud computing environments.

Hashizume et al. analyzed security vulnerabilities in cloud systems and highlighted threats such as insecure APIs and data leakage.

Zissis and Lekkas proposed an encryption-based security architecture for cloud environments.

Ali et al. conducted a comprehensive survey on cloud security risks and categorized major cyber threats affecting cloud platforms.

Modi et al. reviewed intrusion detection techniques designed for cloud environments.

Recent studies focus on machine learning and deep learning- based intrusion detection systems for detecting cyber attacks in cloud networks.

IV. COMPARISON OF EXISTING APPROACHES

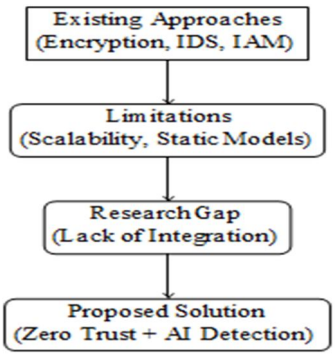


Fig. 2. Research Gap Analysis in Cloud Security

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

V. PROPOSED CLOUD SECURITY ARCHITECTURE

The proposed architecture follows a multi-layered security approach to protect cloud environments from various cyber threats. Each layer is designed to address specific vulnerabilities and provide defense-in-depth.

A. Authentication Layer

This layer implements Multi-Factor Authentication (MFA) to verify user identity. By requiring multiple forms of verification, it significantly reduces the risk of unauthorized access and credential-based attacks.

B. Access Control Layer

The access control layer enforces Zero Trust principles, where no user or system is trusted by default. It applies least privilege access policies to ensure that users only have access to the resources necessary for their roles.

C. Data Security Layer

This layer ensures data confidentiality through encryption mechanisms. Data is encrypted both at rest and during transmission, minimizing the risk of data breaches and unauthorized exposure.

D. Intrusion Detection Layer

An AI-based intrusion detection system is used to monitor system behavior and identify anomalies. Machine learning models such as Random Forest and Support Vector Machines (SVM) are utilized to detect potential cyber threats in real time.

E. Monitoring Layer

The monitoring layer continuously tracks user activities and system logs. It generates alerts for suspicious behavior, enabling quick response to potential security incidents.

F. Security Workflow

The overall workflow of the proposed architecture is as follows:

1) The user initiates a request to access cloud resources.
2) The system verifies the user's identity using Multi-Factor Authentication.
3) Zero Trust policies validate access permissions.
4) Data is encrypted before being transmitted or accessed.
5) The intrusion detection system monitors activity for anomalies.
6) Alerts are generated if suspicious behavior is detected.

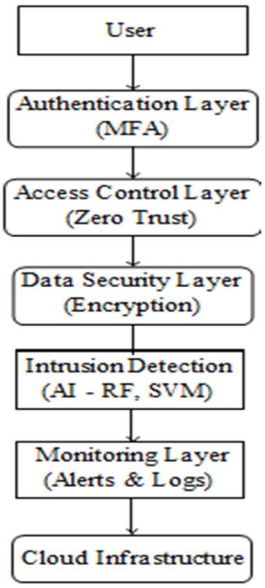


Fig. 3. Proposed Layered Cloud Security Architecture

VI. METHODOLOGY

This study follows a systematic literature review approach. Research papers were collected from IEEE Xplore, Google Scholar, and ScienceDirect databases using keywords such as cloud security, cybersecurity challenges, and intrusion detection in cloud systems. Fifteen research papers were selected based on relevance and publication quality. Each paper was analyzed based on methodology, key findings, and research limitations.

VII. CLOUD SECURITY THREAT TAXONOMY

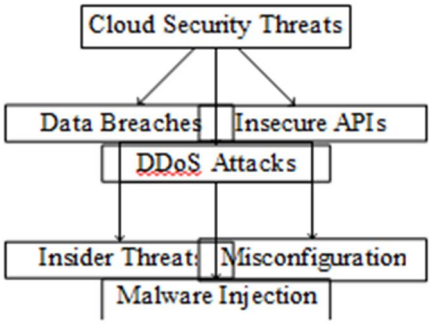


Fig. 4. Taxonomy of Cloud Security Threats

VIII. PROPOSED CLOUD SECURITY ARCHITECTURE

The proposed framework integrates multiple security mechanisms including multi-factor authentication, encryption, and AI-based intrusion detection systems.

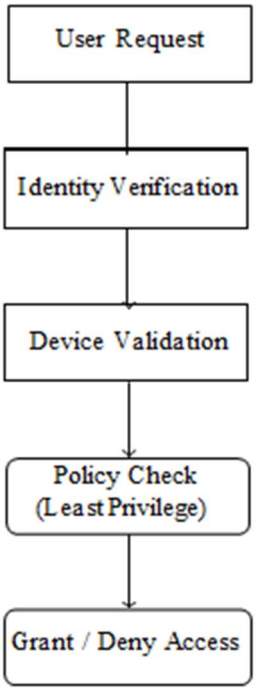
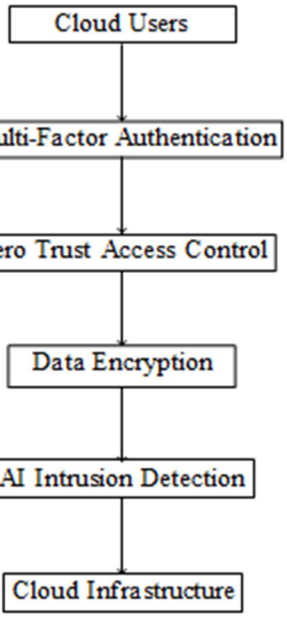
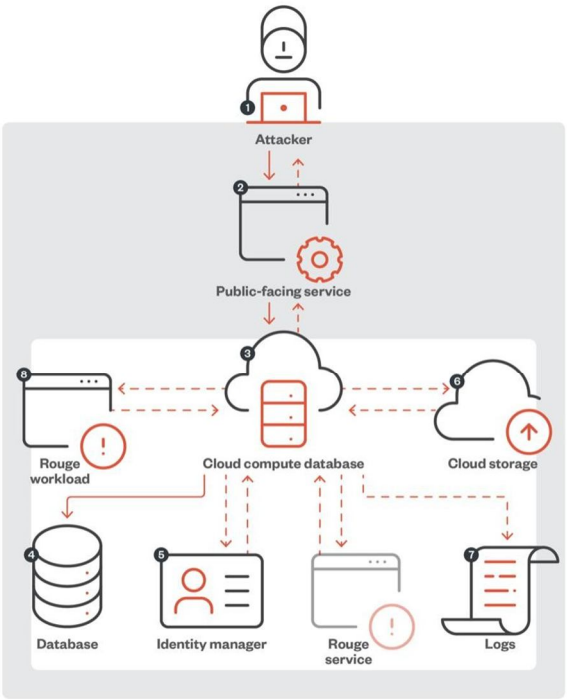


Fig. 5. Zero Trust Access Control Workflow



Proposed Cloud Security Framework



At the core of the taxonomy are data breaches, which represent one of the most critical threats due to their direct impact on sensitive information. These breaches are often caused by misconfigurations, weak authentication mechanisms, or lack of encryption.

Insecure APIs form another major category, as cloud services rely heavily on APIs for communication. Poorly designed or unprotected APIs can expose systems to unauthorized access and data manipulation.

Account hijacking is primarily associated with credential theft through phishing or malware attacks. Once attackers gain access, they can exploit cloud resources and compromise data integrity.

Distributed Denial-of-Service (DDoS) attacks target the availability of cloud services by overwhelming systems with excessive traffic, leading to service disruption.

Insider threats arise from authorized users who misuse their access privileges, either intentionally or unintentionally. These threats are particularly difficult to detect due to legitimate access rights.

Finally, misconfiguration is identified as a cross-cutting issue that contributes to multiple security vulnerabilities. Incorrect settings in storage, access control, or network configurations can significantly increase the attack surface.

This taxonomy highlights that cloud security threats are interconnected, and a single vulnerability can lead to multiple types of attacks. Therefore, a comprehensive and layered security approach is required to effectively mitigate these risks.

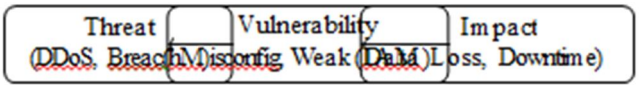


Fig. 7. Relationship between Threats, Vulnerabilities, and Impact

IX. EVALUATION DISCUSSION

Machine learning algorithms such as Random Forest and Support Vector Machines are widely used for intrusion detection in cloud networks. Datasets such as CICIDS2017 and NSL-KDD are commonly used to evaluate security models. Performance metrics such as accuracy, precision, recall, and F1-score are used to measure detection performance.

X. FUTURE RESEARCH DIRECTIONS

Future research should focus on scalable intrusion detection systems for large cloud environments. Blockchain-based security frameworks and privacy-preserving encryption techniques also show promise in improving cloud security. Despite recent progress, cloud security solutions remain limited by scalability, adaptability, and fragmented deployment across layers. Future research should focus on integrated, data-driven approaches that can operate effectively in dynamic, multi-tenant environments.

First, intrusion detection systems need to move beyond static models. While algorithms such as Random Forest and Support Vector Machines provide strong baseline performance, they struggle with evolving attack patterns and large-scale streaming data. Future work should explore online learning and hybrid deep learning models capable of continuous adaptation with low latency.

Second, identity and access management requires stronger contextual awareness. Current Zero Trust implementations rely primarily on static policies. Incorporating behavioral signals (e.g., device posture, access patterns) can enable risk-aware authentication and reduce reliance on binary access decisions. Third, privacy-preserving security mechanisms remain underdeveloped. Techniques such as homomorphic encryption and secure multi-party computation allow computation over encrypted data, but their computational overhead limits practical deployment. Research is needed to optimize these methods for real-time cloud applications.

Fourth, automated response systems should be extended beyond detection. Most current frameworks focus on identifying threats rather than responding to them. Self-healing architectures that isolate compromised components and dynamically reconfigure resources can significantly reduce attack impact. Finally, emerging technologies such as quantum computing pose long-term risks to existing cryptographic standards. Developing and integrating quantum-resistant encryption schemes will be critical for ensuring future-proof cloud security. Overall, future research should prioritize adaptive, scalable, and autonomous security frameworks that combine intelligent detection with real-time response capabilities.

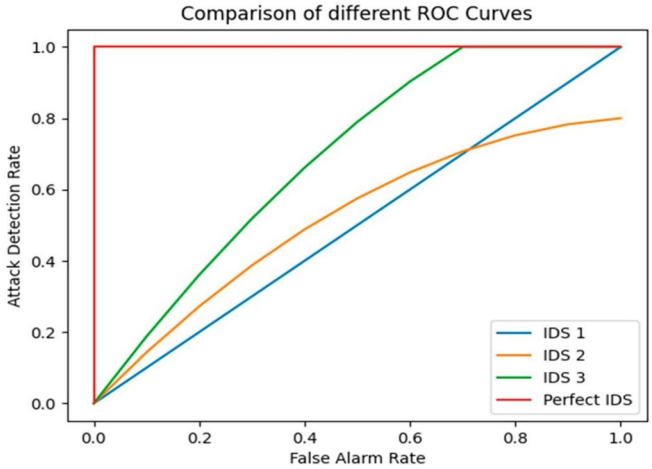


Fig. 8. Comparison of ROC curves for different intrusion detection systems

XI. CONCLUSION

Cloud computing security remains a major challenge due to increasing cyber threats and complex cloud architectures. This paper reviewed existing research and proposed a cybersecurity framework integrating authentication, encryption, and AI-based intrusion detection to improve cloud security. In addition to identifying major cloud security threats, this study highlights the growing importance of integrated and adaptive security mechanisms in modern cloud environments. The analysis demonstrates that relying on isolated security solutions is insufficient to address multi-stage and evolving cyberattacks.

The proposed layered framework emphasizes the need for defense-in-depth, where authentication, access control, data protection, and intrusion detection work together rather than independently. This approach reduces the risk of single points of failure and improves overall system resilience.

Another key observation is the critical role of identity and access management in cloud security. Weak authentication and misconfigured access policies continue to be primary causes of security breaches, indicating that stronger identity-centric security models are necessary.

Furthermore, the incorporation of AI-based intrusion detection enables faster and more accurate identification of anomalies compared to traditional methods. This enhances the system's ability to respond to threats in real time.

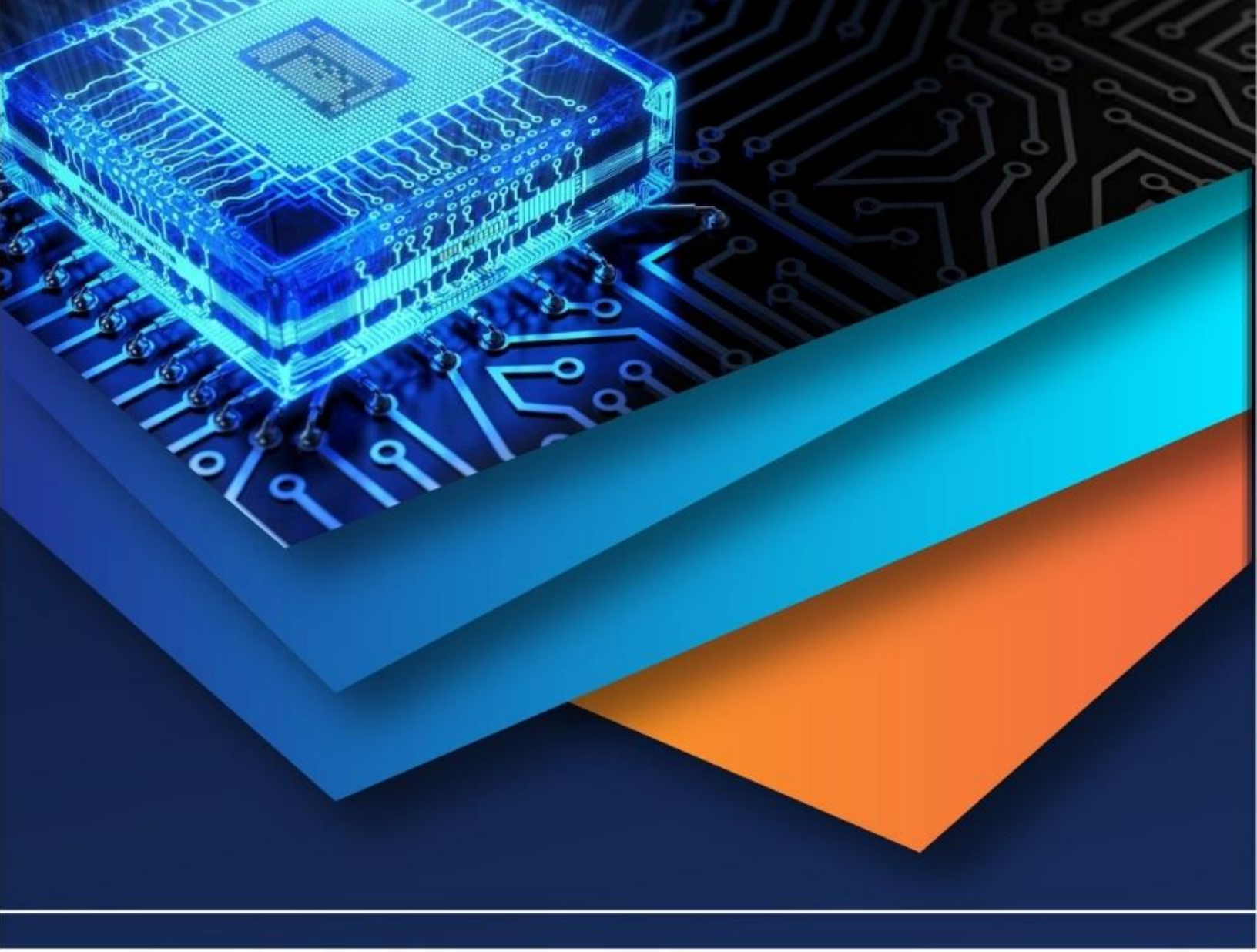
From a practical perspective, the proposed framework can be applied across different cloud service models, including SaaS, PaaS, and IaaS, making it adaptable to various deployment scenarios.

Overall, this work reinforces the need for continuous monitoring, proactive threat detection, and multi-layered protection strategies to secure cloud infrastructures against increasingly sophisticated cyber threats.

As cloud adoption continues to grow, the effectiveness of security frameworks will depend on their ability to evolve alongside emerging threats and technological advancements.

REFERENCES

[1] K. Hashizume et al., "An analysis of security issues for cloud computing," Journal of Internet Services.
[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems.
[3] M. Ali, S. Khan, "Security in cloud computing," Information Sciences.
[4] C. Modi et al., "Intrusion detection techniques in cloud computing," Journal of Network and Computer Applications.
[5] S. Subashini and V. Kavitha, "Security issues in service models of cloud computing," Journal of Network and Computer Applications.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY