A SURVEY OF COMPREHENSIVE SECURITY APPROACHES IN CLOUD COMPUTING: FROM IDS TO LEGAL COMPLIANCE

**Dr. Pradeep Laxkar1**

1 Associate Professor, Department of Computer Science and Engineering, ITM(SLS) University, Vadodara, Gujarat

pradeep.laxkar@gmail.com

Abstract:The revolutionary technology that makes advantage of the internet to supply scalable and reasonably priced computer resources is cloud computing. But as cloud services become more widely used, security, privacy, and regulatory compliance have grown to be major issues. Including technological safeguards such as improved access control techniques, data protection mechanisms, homomorphic encryption, and IDS/IPS, this paper offers a thorough examination of cloud computing security solutions. Other cloud security standards that are analyzed include the NIST Cybersecurity Framework and the Cloud Control Matrix from the Cloud Security Alliance. The article discusses several legal and regulatory issues, including data sovereignty, audits, SLAs, and the shared responsibility paradigm between cloud service providers and clients. This research looks at both technological and legal factors in order to give a thorough knowledge of the strategies required to improve trust, safeguard sensitive data, and guarantee compliance in cloud settings. This demonstrates how applicable and useful the methods are in both local and global settings.

**Keywords:** Cloud Computing Security, Intrusion Detection and Prevention, Data Protection Techniques, Access Control Mechanisms, Legal Compliance in Cloud.

1. INTRODUCTION

Many clients can use IT-enabled capabilities that are highly scalable online as services under the cloud computing paradigm. Among the many benefits offered by these services are business applications, processing power, and storage space. CC is a group of services that are enabled by networks and offer scalable solutions [1][2], which are easy to use, efficient, and reasonably priced. Without being limited by physical infrastructure or location, it enables the on-demand distribution of hardware and software resources. As defined in [3] CC is a computing technology that uses the internet to deliver highly scalable IT-related resources to a range of external clients as a service, redefining the accessibility and dispersion of digital infrastructure.

The use and expansion of cloud computing are significantly impacted by two major concerns: data security and privacy. Numerous security flaws exist in cloud infrastructures due to their remote and multi-tenant nature. Cloud service providers must protect client data from threats such as viruses, unauthorized access, and data breaches [4]. To ease these concerns, providers implement a variety of security policies and practices [5]. However, because cloud infrastructure is shared, there is also a chance that malevolent actors may exploit data. One of the most alluring benefits of cloud computing is the ability to share data across enterprises, but it also brings with it risks that need to be properly addressed. As a result, protecting data repositories ought to be a primary concern for cloud security procedures. In this context, the emphasis is on identifying data security issues, implementing preventive measures, and establishing robust frameworks to safeguard cloud environments.

The average user runs at least four cloud-based apps at any given time and is usually assessing another four, according to a Right Scale poll. Additionally, according to the poll, 41% of businesses use public cloud platforms to handle a significant amount of their burden. Due to such increased reliance on cloud infrastructure, the top priority has been made on the aspect of cloud security [6]. In support of this finding, a 2017 Forbes article noted that 80% of IT spending was anticipated to go toward cloud solutions in less than 15 months. However, it also pointed out that 49% of companies put off implementing cloud computing because of a lack of security expertise and general worries about system integrity and data protection [7]. Since cloud penetration is at a tipping point both at a personal and at a business level, this data shows the necessity to implement better protection and regulatory measures, and quickly.

Besides case of risks associated with technology there are issues of concern relating to cloud computing settings in terms of legal compliance [8]. In India, legal compliance denotes an activity that is dynamic and complex composed of laws, rules and standards governing the actions of corporations. Cloud space businesses must comply with various critical legislations, such as Companies Act of 2013, which governs business creation, reports, and incorporation. The industry also has regulations about banking, telecommunication and insurance related to the industry The working conditions and employee rights to activities like cloud are also covered through employment acts like the Industrial Disputes Act (1947), and the Employees provident funds and Miscellaneous Provisions Act (1952).

The IDS is critical in modern cloud security as it is needed to detect suspicious or unauthorized logins that need to be prevented to protect data. If any activity that threatens system or network integrity is carried out then it can be considered an intrusion. They include attacks over the internet and internal threats where authorized users attempt to leave the abuse of their powers or exceed their limits of accessing the information [9]. A smart way of detecting and preventing such attacks is installing a cloud-based intrusion detection system. Such solutions can minimize risks that land on being serious security breaches, since they monitor cloud configurations in real time [10].

The paper gives an in-depth discussion of cloud security strategies, with the focus on intrusion detection systems and legal compliance strategies. This study will provide an in-depth insight on the technological and legally necessary security involved to make the cloud computing activities secure and legal.

* 1. **Structure of Paper**

The plan of the work is the following: Section II comments on intrusion detection and technical security measures. The description of the levels of cloud security and compliance is provided in Section III. Section IV is the legal and regulatory consideration. Section V summarizes connected literature, and the last Section VI concludes with recommendations of future research.

1. INTRUSION DETECTION AND CORE TECHNICAL SECURITY MEASURES

In order to offer customers a high level of cloud confidence, a safe cloud deployment requires adaptive security measures. Without these methods' capacity to ensure a significant degree of confidentiality and privacy [11], the ongoing concern about sensitive data leaks and privacy loss will be a significant barrier to the full adoption of cloud services.

* 1. **Intrusion Detection and Prevention Systems (IDS/IPS)**

IDS/IPS are essential components in modern cloud security infrastructure [12][13]. IDS examines network traffic and sends out notifications when it detects harmful activities [14]. Once an assault has started, IDS solutions may usually reset TCP connections by sending specially constructed packets. In some situations, they can also communicate with firewall systems to change rulesets on the fly in reaction to threats that are identified.

* + 1. **Intrusion Detection System (IDS)**

IDSs that are standalone devices within a network are called NIDS, whereas those that run on a single workstation are called HIDS. In order to identify such threats, HIDS uses the system's resources to monitor traffic on its host computer. NIDS, on the other hand, monitors all network traffic and operates independently of the devices connected to the network. NIDS are often divided into two categories: Heuristic-based NIDS, which identifies unusual or suspicious behaviour, and signature-based NIDS, which recognizes established attack methods. Each type offers a different level of detection capability and performance efficiency.

* + 1. **Intrusion Prevention Systems (IPS)**

Malicious activity is not only detected by an IPS, but it is also actively blocked or mitigated [15]. It can terminate the network connection or user session associated with an attack and restrict further access by the offending IP address, user account, or other identifiable attributes. IPS can also alter the security environment by modifying configurations of other connected security controls in response to a threat. Furthermore, IPS technologies may sanitize the attack by removing or replacing malicious components to neutralize its effect.

* 1. **Data Protection Techniques**

Authentication, authorization, integrity protection, encryption, and data loss prevention techniques are the best ways to secure data in the cloud. When businesses and suppliers employ cryptographic algorithms [16], according to NIST, these algorithms must be well recognized. The International Journal of Grid and Distributed Computing states that it is also advantageous to review the algorithms and keys that are used annually to ensure the system's security.

* 1. **Homomorphic Encryption and Secure Multiparty Computation**

The foundation of homomorphic encryption is the idea of homomorphism, which allows encrypted data to undergo particular mathematical operations that, when decrypted, provide outcomes identical to those achieved by performing the same operations on the original, unencrypted data. This characteristic allows for computations such as addition, multiplication, and comparison to be conducted directly on encrypted inputs, without revealing their actual content. Homomorphic encryption is consequently quite useful in cases where a sensitive information is to be evaluated or distributed in a secure manner as it allows processing and analysis of data in a safe manner without loss of privacy.

The concept of MPC is used in collaboration with homomorphic encryption to increase data privacy within collaborative settings. In contrast to the conventional data analyses which demand the consolidation of information into a centralized place, MPC enables parties to collaboratively calculate functions over distributed data without revealing the raw information [17]. They are done with specialized cryptography means to guarantee, on the one hand, that every member contributes their data safely and, on the other, that no other participant has access to other parties confidential data. Hence, MPC does not interfere with privacy of individual datasets, as it enables collaborative computation and analysis.

* 1. **Access Control Mechanisms**

One essential security technique used to lessen risks in cloud and Internet of Things systems is access control. [18]. It ensures that system resources are accessed only by authorized users who possess appropriate permissions, roles, capabilities, or attributes. By clearly defining and restricting user privileges, access control safeguards sensitive assets and maintains data integrity, confidentiality, and accountability within distributed systems, lowering the possibility of illegal access and possible resource misuse.

* + 1. **Role-Based Access Control (RBAC)**

One of the earliest and most widely used models of access control is RBAC. It was standardized in 1996 and has been the subject of much research since the early 1990s. Unlike ACLs, which rely on user identity, RBAC makes access decisions based on predefined user roles. As seen in Figure 1, each user (or topic) may be allocated one or more responsibilities. Every position is associated with specific activities that define access rights or permissions.

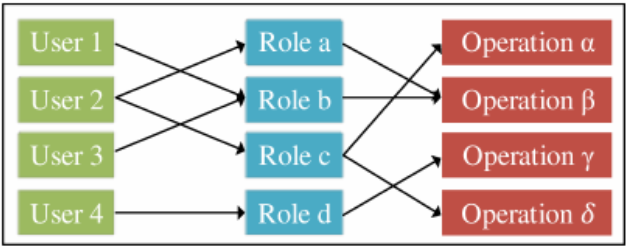


Figure 1: Role-Based Access Control

* + 1. **Attribute-Based Access Control (ABAC)**

The idea of ABAC is to construct an access token by combining the qualities of the user, topic, and environment. As seen in Figure 2, this implies that user roles, user capabilities, and access permissions are all taken into account as characteristics and utilized when making access decisions. When access is requested, After then, this access token is compared to one or more remote or local access regulations.

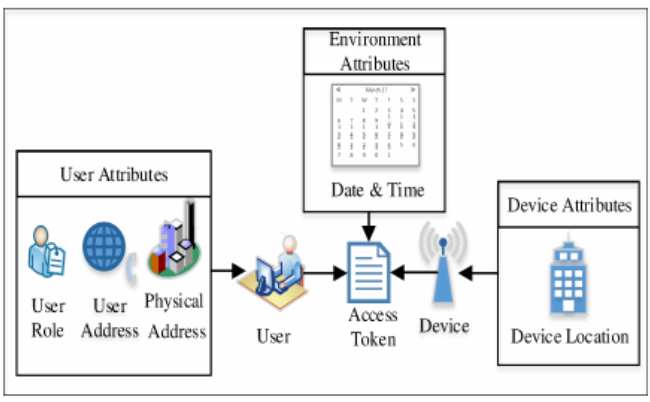


Figure 2: Attribute-Based Access Control

* + 1. **Relationship-Based Access Control (ReBAC)**

One of the most recent access control techniques to be created is ReBAC. The concept of a binary relationship manager is introduced by this approach. ReBAC employs a binary connection between the asset and the accessor in place of a unary predicate based on identity, role, or attribute. Figure 3 illustrates how ReBAC is utilized in social media applications like Facebook. An example of U2U relationship access control is shown in the right portion of the picture, where access is only permitted if the activity conforms with additional access control rules and the asset (the second friend) and the accessor (the first friend) are friends [19].

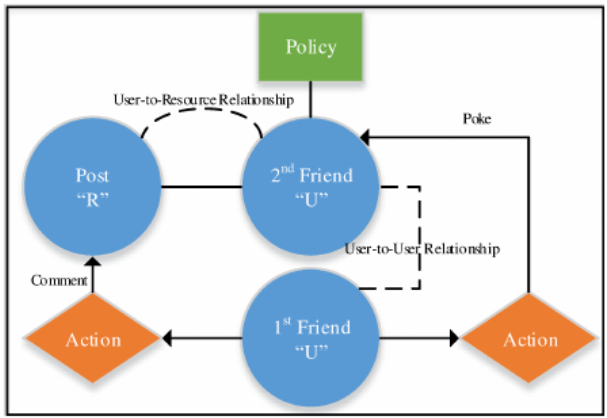


Figure 3: Relationship-Based Access Control

1. CLOUD SECURITY STANDARDS AND COMPLIANCE

A key component of this security control is cloud security and compliance, which uses a semantic approach to end-to-end security and includes 485 authorized users [20]. Passwords and Key Management are Needed for Users' Identification. In order for other authorized users to be granted rights, cloud providers should also grant users access controls.

The primary threats to cloud security are as follows:

* Data breaches impact data confidentiality and ultimately the organization. The information is encrypted so that even if it is stolen, the attacker cannot use it.
* Malicious assaults on the system or hardware malfunctions might cause data loss. To combat such threats, data backup policies have to be implemented.
* User confidentiality and integrity are jeopardized when accounts or services are traffic hijacked. User information, including bank login details, can be stolen by hackers. To lower these, fraud detection and anti-phishing procedures need to be put in place.
* APIs and insecure interfaces: These technologies help users and providers communicate. Data should be able to be encrypted before being sent over APIs.
* A denial of service attack is used to prevent authorized users from accessing their data. The attacker can alter the encryption key or slow down the system to prevent users from using the service.
  1. **NIST Cybersecurity Framework (CSF)**

The Framework Core, Framework Implementation Tiers, and Framework Profiles comprise the NIST CSF. Identify, Protect, Detect, Respond, and Recover are the five continuous and concurrent functions that make up the Framework Core. It created an assessment technique for their inquiry based on these features, which offered a methodical way to determine the company's cybersecurity risk management procedures and guidelines [21].

The tier levels are described as follows:

* **Tier-1 (Partial):** In this stage, risk management is largely unstructured and reactive. Organization-wide cybersecurity awareness is minimal, and collaboration with external stakeholders is rarely established or systematically approached.
* **Tier-2 (Risk Informed):** Risk-based decisions begin to shape cybersecurity activities, supported by formal yet siloed processes. Internal and external communication exists but relies on informal methods, limiting consistent cybersecurity awareness and response.
* **Tier-3 (Repeatable):** At this maturity level, comprehensive policies and structured processes guide risk management [22]. A consistent organizational framework supports cybersecurity, leveraging skilled staff and well-understood interdependencies with external entities.
* **Tier-4 (Adaptive):** Cybersecurity protocols prioritize quick response, adaptability, and continuous improvement and are based on anticipated indicators and lessons gained. One aspect of the organizational culture that is regularly communicated to external partners is the organization-wide approach to controlling cybersecurity threats.
  1. **Cloud Security Standards and Certifications**

For CSPs to adhere to industry-accepted security practices and legal obligations, cloud security standards and certifications are crucial [23]. These frameworks help manage data confidentiality, integrity, and availability across cloud environments. ISO/IEC 27017 for cloud-specific controls and same for information security management are significant standards. Certifications such as SOC 2, CSA STAR, and FedRAMP demonstrate compliance with stringent security requirements. Adherence to these standards enhances trust, ensures accountability, and supports informed provider selection through standardized assessments.

1. LEGAL AND REGULATORY CONSIDERATIONS
   1. **Data Sovereignty and Jurisdiction**

The idea that information is governed by the political and legal system of the country in which it is gathered or held is known as data sovereignty. Data in cloud computing frequently exists in several places across several nations [24], leading to complex jurisdictional challenges.

* **International Regulations:** Legal frameworks like the GDPR have attempted to harmonies data protection laws across member states, reducing some jurisdictional issues. However, challenges remain, especially when data is transferred to countries outside these frameworks [25].
  1. **Cloud Service Level Agreements (SLAs)**

As seen in Figure 4, Service Level Agreements (SLAs) are official contracts that outline the expected level of service, obligations, and recourse in the event of service failures between clients and cloud service providers (CSPs).

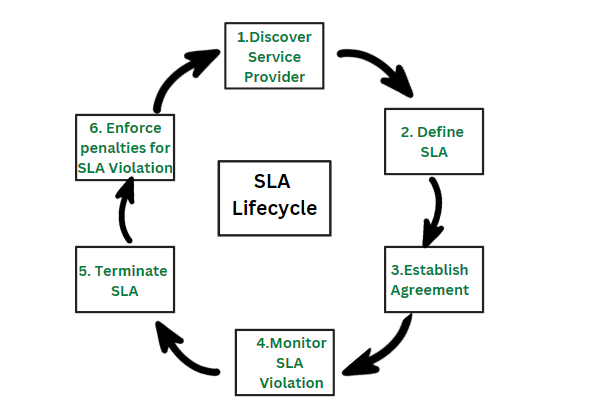


Figure 4: SLA life cycle

* **Legal Binding and Limitations:** SLAs are legally binding contracts. However, analyses have shown that many cloud providers include broad disclaimers of liability and warranties, often limiting remedies to service credits. This can leave clients with limited recourse in the event of service outages or breaches [26].
* **Security and Privacy Metrics:** Modern SLAs are evolving to include security and privacy metrics, addressing concerns over data protection. These metrics help in defining clear expectations and responsibilities regarding data security.
* **Third-Party Auditing:** To ensure compliance with SLAs, third-party auditing mechanisms are recommended. These audits can verify whether the service provider meets the agreed-upon performance and security standards.
  1. **Auditing and Legal Disclosure Requirements**

In cloud computing, auditing involves a systematic overlapping of practices and systems to facilitate compliance with the law and regulations. The legal disclosure requirements address the necessity of CSPs to inform authorities in particular situations.

* **Continuous Auditing:** The embrace of continuous auditing methodology would enable auditing of the cloud services in real-time, which promotes transparency and compliance. Techniques such as XBRL can assist in the building of continuous auditing modules with the help of standard method of marking and processing of data.
* **Legal Disclosure:** According to the U.S. CLOUD Act and other laws, federal law-enforcement authorities may demand that U.S.-based technology companies disclose requested data stored on servers whether they are located in the United States or not. This has significant implications to data stored on clouds because it may become subject of cross-border legal requests.
  1. **CSPs Responsibilities vs. Clients Responsibilities**

The number of responsibilities allocated to the client and CSP is predetermined by the number of control rights, where both of them are defined by cloud service model.

* **Shared Responsibility Model:** CSPs will normally be in charge of cloud infrastructure and ensuring its safety by taking precautionary measures, and clients must additionally take necessary measures to protect their data in cloud. The relationships between the involved entities in this model shall be well-defined in terms of responsibilities to ensure there is no loose end in terms of security, and other compliances.
* **Compliance with Regulations:** Clients and CSPs both have the responsibility to ensure that relevant data protection regulations are observed. To give a clear example, the GDPR mandates CSPs who process the data to ensure they establish the right organizational and technological protection mechanisms to protect personal data.

work, typically using web services [

84

]. Most modern web APIs

comply with the REST architectural style [

74

], being referred to as

RESTful web APIs. RESTful web APIs [

95

] Provide access to data

and services by means of create, read, update, and delete (CRUD)

operations over resources (e.g., a video in the YouTube API [

50

] or

a playlist in the Spotify API [

44

]). RESTful APIs are ubiquitous in

the modern-day society: public institutions such as the American

government [

3

] expose their existing assets as a set of RESTful

APIs; software companies such as Microsoft [

29

] and Netix [

30

]

base many of their systems communications on their RESTful APIs;

even non-software companies such as Marvel [

28

] provide APIs for

developers to build applications on top of them. The importance and

pervasiveness of web APIs is also reected on the size of popular

API repositories such as ProgrammableWeb [

37

] and RapidAPI [

38

],

which currently indexes over 24K and 30K APIs, respectively.

1. LITERATURE REVIEW

This section on Literature Review contains recent developments on cloud and IoT security in terms of risk analysis, intrusion detection, and secure access. It highlights AI-driven solutions, key challenges, and potential directions for enhancing system resilience and performance.

Drissi, Chergui, and Khatar (2025) examined the latest developments in cloud computing security in detail, with an emphasis on RA, was the main goal of the systematic literature study. In order to detect and reduce any dangers in cloud settings, their study also investigates a variety of RA scenarios using ML and DL approaches. This research addresses the unique features of the cloud and its complexity while highlighting the most recent approaches to risk assessment in the cloud. This helps to build a thorough RA. It also discusses how future research will improve RA based on a variety of parameters [27].

Than, Soe, and Maw (2024) intended to investigate two oversampling strategies, SMOTE and ADASYN, in order to enhance classification performance in IoT-IDS. The KDDCUP-99 and IoT2020 dataset’s class imbalance was addressed using four machine learning methods. The evaluation computes F1-score, accuracy, recall, and precision. [28].

Reddy et al. (2023) utilized the shared responsibility concept in public cloud systems. The cloud has several problems with safe data access and storage, despite its many advantages and services. Cloud security has a number of problems, including carrier disruption, data loss, loss of control, vendor lock-in, and multi-tenancy. The main cloud issues are examined in this paper along with solutions. Data loss has been deemed a significant concern in this study, which also examines several methods for safeguarding data in the cloud through the use of encryption algorithms and authentication [29].

Tayouri et al. (2022) highlighted safe remote access in their presentation on cloud security best practices and standards. Availability of services and applications, many of which are stored on the cloud, is necessary for digital business transformation. These days, the corporate perimeter, a dynamic, policy-based secure access service edge, can be found anywhere. Businesses wish to safeguard their resources from unauthorized parties. However, by enabling users and dependable devices to access on-premises or cloud-based apps, they also hope to maintain business continuity. Secure remote access is one of the most important security layers to do this [30].

Kiran (2022) suggested DWA-IDS as a WPS attack intrusion detection solution. For simulation, they use the Contiki-cooja simulator. The simulation's findings show that by increasing packet transmission delays, the WPS attack lowers system performance. The DWA-IDS simulation results demonstrate that their IDS can identify any hostile node that initiates a WPS assault. The suggested DWA-IDS has a 100% detection rate and a true positive rate of over 95%. Furthermore, because their DWA-IDS does not contain false-positive cases, it offers the theoretical justification for the false-positive scenario. DWA-IDS's reduced overhead makes it possible to set up devices with constrained power and memory [31].

Table 1 provides a comparative overview of recent studies addressing cloud and IoT security, highlighting methodologies, key findings, prevailing challenges, and future research directions to enhance system protection and resilience.

Table 1: Summary of Related Work on Cloud Computing on IDS to Legal Compliance

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Authors** | **Study On** | **Approach** | **Key Findings** | **Challenges** | **Future Discussions** |
| Drissi, Chergui & Khatar (2025) | Cloud Risk Assessment (RA) using ML/DL | Systematic Literature Review of RA methods in cloud environments with ML/DL integration | Highlights latest RA techniques using AI, improving cloud security understanding | Complexity of cloud architecture and adaptability of AI techniques | Enhance RA frameworks using adaptive AI and multi-criteria decision-making |
| Than, Soe & Maw (2024) | Imbalanced Classification in IoT-IDS | SMOTE & ADASYN with 4 ML algorithms on KDDCUP-99 & IoT2020 datasets | Improved classification metrics (accuracy, F1-score, etc.) in IDS for IoT | Handling class imbalance effectively | Expand dataset variety and ensemble-based IDS approaches |
| Reddy et al. (2023) | Cloud Security Challenges | Review of security concerns & mitigation techniques in public cloud | Identified key threats like data loss, vendor lock-in, proposed authentication & encryption methods | Trust management, data control, and multi-tenancy risks | Propose robust data protection frameworks across hybrid cloud environments |
| Tayouri et al. (2022) | Secure Remote Access in Cloud | Cloud security guidelines & practices for distributed access | Emphasized SASE and policy-based access for remote digital transformation | Balancing security and access across hybrid infrastructures | Develop adaptive secure remote access models integrating AI/ML |
| Kiran (2022) | WPS Attack Detection via IDS | DWA-IDS implemented on Contiki-Cooja for IoT networks | Achieved >95% true positive rate; 100% detection rate; no false positives | System performance under WPS attack; resource limitations | Optimize IDS for energy-constrained IoT setups and wider threat models |

1. CONCLUSION AND FUTURE WORK

CC is still transforming the IT industry by offering flexible, affordable, and scalable data processing and storage options. However, there are serious issues with data security, privacy, and legal compliance that arise with its extensive use. In addition to following well-known cloud security guidelines like the CSA Cloud Control Matrix and NIST Cybersecurity Framework, this report emphasizes the necessity of putting strong technological security measures in place, such as IDS/IPS, encryption, and access control. Moreover, legal considerations, including data sovereignty, service-level agreements, and shared responsibilities between cloud providers and clients, must be carefully managed to avoid compliance breaches and jurisdictional conflicts. By integrating technical and regulatory approaches, cloud stakeholders can build secure, transparent, and legally resilient cloud environments. Future research should continue to bridge the gap between technology and law, especially as cloud infrastructures evolve and regulatory landscapes become increasingly complex.

In future, researchers must focus on developing automatic and intelligent security models that rely on AI and machine learning to detect and react to threats in cloud environments in real time. Additionally, enhancing cross-border legal frameworks and harmonizing data protection laws will be crucial to address jurisdictional challenges. Exploring privacy-preserving technologies such as federated learning and zero-knowledge proofs can further strengthen data security in multi-tenant cloud architectures.

REFERENCES

[1] S. P. Bheri and G. Modalavalasa, “Advancements in Cloud Computing for Scalable Web Development: Security Challenges and Performance Optimization,” *JCT Publ.*, vol. 13, no. 12, pp. 01–07, 2024.

[2] S. Garg, “Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations,” *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[3] C. Chimonaki, S. Papadakis, K. Vergos, and A. Shahgholian, “Identification of Financial Statement Fraud in Greece by Using Computational Intelligence Techniques,” in *Lecture Notes in Business Information Processing*, 2019, pp. 39–51. doi: 10.1007/978-3-030-19037-8\_3.

[4] V. Prajapati, “Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study,” *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[5] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *J. Supercomput.*, 2020, doi: 10.1007/s11227-020-03213-1.

[6] A. K. Polinati, “Hybrid Cloud Security: Balancing Performance, Cost, and Compliance in Multi-Cloud Deployments,” pp. 1–24, 2025, doi: 10.48550/arXiv.2506.00426.

[7] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, “A survey on security in internet of things with a focus on the impact of emerging technologies,” *Internet of Things (Netherlands)*. 2022. doi: 10.1016/j.iot.2022.100564.

[8] S. B. Shah, “Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure,” *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

[9] N. K. Prajapati, “Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection,” *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[10] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, “Dynamic defenses in cyber security: Techniques, methods and challenges,” *Digit. Commun. Networks*, 2022, doi: 10.1016/j.dcan.2021.07.006.

[11] Y. S. Abdulsalam and M. Hedabou, “Security and privacy in cloud computing: Technical review,” *Future Internet*. 2022. doi: 10.3390/fi14010011.

[12] G. Modalavalasa and S. Pillai, “Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security,” *ESP J. Eng. Technol. Adv.*, vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.

[13] V. Prajapati, “Cloud-Based Database Management: Architecture, Security, challenges and solutions,” *J. Glob. Res. Electron. Commun.*, vol. 01, no. 1, pp. 07–13, 2025.

[14] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, “Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS),” *Glob. J. Eng. Technol. Adv.*, vol. 14, no. 2, pp. 155–158, Feb. 2023, doi: 10.30574/gjeta.2023.14.2.0031.

[15] A. K. Polinati, “AI-Powered Anomaly Detection in Cybersecurity: Leveraging Deep Learning for Intrusion Prevention,” *Int. J. Commun. Networks Inf. Secur.*, vol. 17, no. 3, 2025.

[16] K. Jakimoski, “Security techniques for data protection in cloud computing,” *Int. J. Grid Distrib. Comput.*, 2016, doi: 10.14257/ijgdc.2016.9.1.05.

[17] S. Bhaskar, K. Parmar, and D. C. Jinwala, “A Survey of Ciphertext Processing Techniques,” in *Lecture Notes in Electrical Engineering*, 2022, pp. 735–747. doi: 10.1007/978-981-19-5037-7\_53.

[18] H. S. Chandu, “A Review of IoT-Based Home Security Solutions: Focusing on Arduino Applications,” *TIJER – Int. Res. J.*, vol. 11, no. 10, pp. a391–a396, 2024.

[19] M. Alramadhan and K. Sha, “An overview of access control mechanisms for internet of things,” in *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*, 2017. doi: 10.1109/ICCCN.2017.8038503.

[20] R. Kalaiprasath, R. Elankavi, and R. Udayakumar, “Cloud security and compliance - A semantic approach in end to end security,” *Int. J. Smart Sens. Intell. Syst.*, 2017, doi: 10.21307/ijssis-2017-265.

[21] H. Kali, “The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday,” *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, 2023.

[22] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, “A security review of local government using NIST CSF: a case study,” *J. Supercomput.*, 2018, doi: 10.1007/s11227-018-2479-2.

[23] Abhishek and P. Khare, “Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development,” *Int. J. Curr. Eng. Technol.*, vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.

[24] P. Chatterjee and A. Das, “AI-Powered Anomaly Detection for Real-Time Performance Monitoring in Cloud Systems,” *Int. J. Sci. Res. Sci. Technol.*, vol. 11, no. 6, pp. 592–601, Dec. 2024, doi: 10.32628/IJSRST241161111.

[25] E. Celeste and F. Fabbrini, “Competing Jurisdictions: Data Privacy Across the Borders,” in *Palgrave Studies in Digital Business and Enabling Technologies*, 2021. doi: 10.1007/978-3-030-54660-1\_3.

[26] A. J. Ferrer and E. P. I. Montanera, “The Role of SLAs in Building a Trusted Cloud for Europe,” in *9th IFIP International Conference on Trust Management (TM)*, 2016. doi: 10.1007/978-3-319-18491-3\_22.

[27] S. Drissi, M. Chergui, and Z. Khatar, “A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements,” *IEEE Access*, vol. 13, pp. 76289–76307, 2025, doi: 10.1109/ACCESS.2025.3561123.

[28] S. S. M. Than, A. M. Soe, and A. H. Maw, “Investigation of Oversampling in IoT-IDS,” in *2024 IEEE Conference on Computer Applications (ICCA)*, IEEE, Mar. 2024, pp. 1–6. doi: 10.1109/ICCA62361.2024.10533055.

[29] M. V. Reddy, P. S. Charan, D. Devisaran, R. Shankar, and P. M. Ashok Kumar, “A Systematic Approach towards Security Concerns in Cloud,” in *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, 2023, pp. 838–843. doi: 10.1109/ICEARS56392.2023.10085437.

[30] D. Tayouri, S. Hassidim, A. Smirnov, and A. Shabtai, “Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access,” *Cybersecurity Agil. Cloud Comput. Guidel. Cloud Access*, pp. 1–36, 2022.

[31] U. Kiran, “IDS to Detect Worst Parent Selection Attack in RPL-Based IoT Network,” in *2022 14th International Conference on COMmunication Systems and NETworkS, COMSNETS 2022*, 2022. doi: 10.1109/COMSNETS53615.2022.9668340.