

Enhancing Cloud Security: Analysis of Vulnerabilities and a Resilient Framework Proposal

Francis K. Mupila¹, Himanshu Gupta² and Akashdeep Bhardwarj³

¹⁻²Amity University/Amity Institute of Information Technology, Noida, India

Email: kmf.mupila@gmail.com, hgupta@amity.edu

³University of Petroleum and Energy Studies (UPES)/School of Computer Science (Cybersecurity and Digital Forensics), Dehradun, India

Email: abhardwaj@ddn.upes.ac.in

Abstract—This study examines vulnerabilities in cloud security configurations, focusing on commonly implemented authentication mechanisms, access control models, and adaptive security measures. Utilising a large dataset of cloud configurations, we applied descriptive and correlation analyses to identify patterns and associations among crucial security features. Based on their Security Scores, a threshold-based classification method was employed to categorise configurations as high-risk or low-risk. Key findings reveal that configurations lacking multi-factor authentication, granular access controls, and geolocation restrictions are significantly more vulnerable. This study concludes with targeted recommendations, emphasising the need for adaptive controls and Zero-Trust principles to mitigate prevalent risks. Our analysis contributes to developing more resilient cloud environments by identifying critical gaps in traditional security configurations.

Index Terms—Cloud Security, Role-Based Access Control, Multi-Factor Authentication, Zero-Trust, Dynamic Access Management.

I. INTRODUCTION

The widespread implementation of cloud computing has revolutionised data management and service provision across sectors, facilitating scalable, adaptable, and economical solutions for enterprises. Security concerns have intensified as organisations migrate sensitive data and essential apps to the cloud. Cloud environments inherently present new risks, such as multi-tenant vulnerabilities, data breaches, illegal access, and difficulties maintaining regulatory compliance.

These threats underscore the inadequacies of traditional security methods, which frequently need to adapt to the evolving landscape of cloud infrastructure [1].

Previously, cloud security frameworks primarily depended on methods like role-based access control (RBAC) and multi-factor authentication (MFA) to protect data access and verify user identity. Although these systems provide a fundamental level of security, they demonstrate considerable limitations. RBAC, for example, allocates access according to user roles, which may be excessively restricted or unnecessarily expansive, neglecting to consider nuanced access requirements or changeable risk considerations. Multi-factor authentication (MFA) introduces an extra layer of authentication. However, it persists as a static solution in some implementations without the flexibility and agility required to address real-time security threats [2].

As a result, these models may render cloud-based applications susceptible to unauthorised access, privilege escalation, and diverse cyber threats [3].

Given these obstacles, this study aims to discover vulnerabilities in existing cloud security models by thoroughly analysing access control setups and security scores. We strive to identify vulnerabilities and significant deficiencies in existing models by utilising an extensive dataset from Kaggle that reflects actual access patterns, security mechanisms, and corresponding security scores. We present a conceptual framework to solve the reported vulnerabilities, combining dynamic access control and zero-trust ideas. Our proposed approach intends to improve conventional security frameworks in the following manners:

- We combine role-based access control (RBAC) with attribute-based access control (ABAC) to deliver a more precise and flexible access control solution.
- We have introduced compulsory multi-factor authentication for all privileged access points to strengthen defences against unauthorised access.
- We use Zero-Trust principles that consistently authenticate each access request, ensuring real-time security flexibility [4].
- We employ dynamic access management, which adjusts permissions based on real-time user activities and contextual data [5].

The study is critical because it looks at cloud security from a proactive point of view using both dataset-driven vulnerability analysis and a conceptual framework based on best practices. This strategy boosts adaptability, improves real-time threat response, and minimises potential exposure to unauthorised access in cloud environments by addressing critical limitations in existing security configurations.

In an age where cloud-based applications are essential infrastructure for sectors such as healthcare and finance, this study's findings have practical implications for enhancing the security posture of cloud environments. This study and its proposed approach aim to deliver a resilient, flexible, and robust solution for cloud security, effectively aligning security practices with the requirements of contemporary, high-availability cloud services.

II. RELATED WORK AND BACKGROUND

Cloud security has significantly evolved to tackle the rising obstacles of data confidentiality, integrity, and accessibility in cloud systems. Existing security frameworks such as Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and Zero-Trust Architecture offer essential safeguards but encounter limitations in dynamic, multi-tenant settings. Recent studies have explored how technologies such as Artificial Intelligence (AI) and blockchain may mitigate these limitations, promoting more adaptable and resilient security methods for cloud infrastructure [6].

Role-Based and Attribute-Based Access Control (RBAC and ABAC): Access control in cloud settings traditionally depends on role-based access control (RBAC), wherein permissions are allocated according to established user roles. Although efficient in controlled settings, RBAC must improve its adaptability for complex, real-time access requirements. Attribute-Based Access Control (ABAC) introduces a level of granularity by permitting access depending on several variables, including user location and device kind. Even so, ABAC is constrained in its adaptability, as it generally necessitates pre-established rules and needs more capacity for real-time modifications.

Multi-Factor Authentication (MFA) is extensively implemented to enhance security by requiring users to authenticate their identities using different credentials. While MFA enhances authentication, it might be excessively static, failing to adapt dynamically to the changing landscape of threats. MFA alone is frequently inadequate in high-risk situations, requiring additional safeguards against progressively advanced threats, including privilege escalation and session hijacking.

Zero-Trust Architecture: The Zero-Trust architecture has garnered attention for its basic concept of "never trust, always verify," which perpetually authenticates each access request. This method minimises certain dangers linked to static access control but necessitates additional integration with adaptive security mechanisms to address emergent threats dynamically.

In the recent research by Olabanji et al. [7], they investigate AI's capacity to improve Identity and Access Management (IAM) within cloud systems. Their research illustrates that AI can enhance user authentication and authorisation by reacting to real-time threats and increasing flexibility in access control. Utilising machine learning for behavioural analysis, AI can detect abnormal activities, augmenting security beyond conventional IAM systems' limitations.

This strategy corresponds with the objectives of our proposed model, which aims to integrate real-time flexibility into cloud security through dynamic access management.

Furthermore, Khan et al. [8] Investigate the application of blockchain and artificial intelligence in improving access control systems. Blockchain's decentralised ledger enhances accountability and prevents manipulation by establishing an immutable record of access events. When integrated with AI-driven anomaly detection, this approach improves security by eliminating single points of failure and reacting to possible attacks in real-time. Their findings endorse the feasibility of integrating AI with decentralised systems, a principle that motivates our framework's focus on dynamic, resilient security.

Moreover, Kandolo's [9] review highlights AI's efficacy in establishing adaptive security models within relational databases despite its emphasis on RDBMS. The research also highlights AI's significance in facilitating context-aware access control, which adaptively modifies permissions according to user behaviour and location variables. This model underscores the necessity for real-time adaptation in cloud security approaches, prompting our suggestion to incorporate AI-driven dynamic access management within a Zero-Trust framework.

A. Research Gap and Motivation

Although AI and blockchain can improve cloud security, existing implementations remain constrained, especially with dynamic access control. Static solutions of RBAC, ABAC, and MFA frequently need to be more robust in multi-tenant, high-availability settings, where risks proliferate and regulatory compliance introduces complexity. These difficulties highlight the need for more flexible systems that can react to varying user access needs and context-specific requirements in real time.

Our work utilises an extensive dataset of access control configurations to address this deficiency, enabling us to recognise particular weaknesses and patterns of vulnerability within current methods. Based on these results, we suggest a way of thinking that combines the good things about RBAC and ABAC, requires multi-factor authentication (MFA) for special access, and builds dynamic access management into a zero-trust architecture. Our framework's innovative approach prioritises real-time adaptability, reduced vulnerability to unauthorised access, and an enhanced security posture for cloud-based applications.

III. METHODOLOGY AND DATASWT ANALYSIS

This study utilises a comprehensive dataset from Kaggle, encompassing various access control configurations, authentication mechanisms, and security scores for cloud-based applications. The primary objective of this analysis is to identify vulnerabilities within cloud security configurations and suggest improvements. Key features in the dataset include:

- Authentication Mechanisms: include password-only, Multi-Factor Authentication (MFA), and Single Sign-On (SSO) methods.
- Authorisation Models: Methods like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).
- Security Score: A numerical indicator representing the security robustness of each configuration, which serves as the primary outcome variable.

The dataset comprises over 100,000 records and 52 features, providing various configurations across cloud environments. Despite being extensive, the dataset might have limitations due to the particular configurations and providers represented, which could limit the generalizability of findings. Nevertheless, the diversity within the dataset supports a comprehensive analysis of common security vulnerabilities associated with various access control setups.

A. Analytical Approach

A combination of descriptive and correlation analyses was employed to assess configuration trends and uncover potential security risks.

Descriptive Statistics analysis provided an initial overview of distribution patterns in authentication mechanisms, authorisation models, and access levels within the dataset. This approach was chosen to reveal the prevalence of various security practices, offering a foundational understanding that guided further, more targeted analyses.

Correlation Analysis/Correlation coefficients were calculated between features (such as Multi-Factor Authentication [MFA] and access control granularity) to examine associations with security scores. This method was selected to determine whether individual features significantly impacted security outcomes. Low correlation values indicated that isolated features might not account for variations in security scores, suggesting a need for integrated analysis to identify multi-dimensional risk factors.

B. Machine Learning Techniques

Machine learning techniques were applied to gain further insights into feature importance and high-risk patterns:

Feature Importance (Random Forest): A Random Forest model was used to evaluate the impact of various features on the Security Score. This technique was selected for its ability to handle large datasets and identify the most influential security elements, providing insight into which features contribute most to securing cloud configurations.

Clustering Analysis (K-means): K-means clustering grouped configurations based on their security attributes, revealing high-risk and low-risk configuration clusters. This method was chosen to identify patterns of shared vulnerabilities in high-risk configurations, offering a data-driven approach to uncover configurations lacking essential security controls.

C. Threshold-Based Classification

A threshold-based classification approach was applied to the Security Score to categorise configurations as high-risk or low-risk. Configurations with scores above 3.80 were labelled as low-risk, while those below were considered high-risk. This method was chosen for its simplicity and interpretability, providing a direct means to segment configurations based on inherent security levels without the complexity of model training. This approach aligns well with the dataset's nature and the study's objective of identifying clear patterns in configuration risk.

Combining exploratory and confirmatory analyses was an excellent way to find holes in cloud security configurations and help people devise ways to improve them. While the methodology provides a robust analysis of cloud security configurations, future research could expand by incorporating more diverse datasets to generalise findings across cloud service providers.

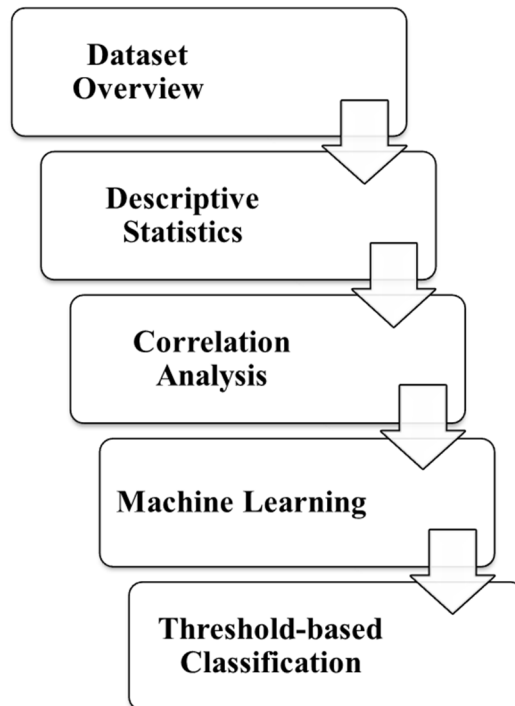


Fig 1: Methodology Process Flow

Fig 1: Methodology Process Flow. This flowchart outlines the sequence of analytical steps taken in the study, starting with the dataset overview and descriptive statistics. The process then proceeds to correlation analysis and clustering to uncover feature relationships and group configurations according to risk level. Finally, the study employs threshold-based classification to interpret and summarise the findings, leading to insights into critical security weaknesses.

IV. FINDINGS & ANALYSIS RESULTS

This section presents the findings from the analysis of cloud security configurations, focusing on identifying critical vulnerabilities in conventional models. It highlights vital security limitations and opportunities for improvement through descriptive statistics, correlation analysis, and machine learning techniques.

A. Analytical Techniques Overview

To evaluate the security of cloud configurations, we applied a combination of analytical methods.

Descriptive Statistics: The first analysis gave a broad picture of security configuration patterns, like how they were spread across authentication mechanisms and access control levels, setting baseline trends in the dataset.

Correlation Analysis: The correlation coefficients between security features (for example, the level of access control and the presence of multi-factor authentication (MFA)) showed that one feature is not sufficient to guarantee that security works. The results indicated that effective security management often requires a combination of features rather than reliance on single components.

Machine Learning Techniques: Further insights into high-risk patterns and influential security features were provided through machine learning, where Random Forest Algorithm analysis identified Geolocation Restrictions, User Roles, Access Levels, Data Sensitivity Classification, and Authentication Mechanisms as the most impactful features for the Security Score, with Geolocation Restrictions and User Roles being top contributors. Consequently, the K-means Clustering method grouped configurations into high-risk and low-risk clusters, revealing that high-risk configurations often lacked strict geolocation and access controls. Furthermore, the Threshold-Based Classification A threshold on the Security Score marked about 17.7% of high-risk configurations. It shows that weak access control and no multi-layered authentication are linked to more security holes. These methods collectively revealed crucial areas for enhancement in cloud security configurations.

B. Key Findings from Descriptive and Correlation Analysis

The analysis identified significant patterns related to key security features:

Authentication Mechanisms and Access Levels. Balanced distribution across authentication types (e.g., password-only, MFA, SSO, and biometrics) showed varied security practices. However, configurations relying solely on password authentication were frequently associated with lower security scores, emphasising the added security benefit of MFA.

Access Control Granularity: Configurations implementing Attribute-Based Access Control (ABAC) showed enhanced security scores over Role-Based Access Control (RBAC))-only setups. ABAC's flexibility, accounting for contextual factors such as user attributes and environmental conditions, mitigated vulnerabilities inherent in static access models.

C. Insights from Machine Learning

Machine learning analyses provided additional insights into feature relevance and risk patterns:

Feature Importance (Random Forest): Geolocation Restrictions, User Roles, Access Levels, Data Sensitivity Classification, and Authentication Mechanisms were identified as the most impactful features for higher security scores. Configurations with well-defined geolocation controls and structured user roles demonstrated greater security resilience.

Risk Level Clustering (K-means): Clustering analysis revealed two primary groups—high-risk and low-risk configurations. High-risk clusters, identified by weaker geolocation restrictions and limited access control, underscored the need for adaptable controls to reduce vulnerabilities.

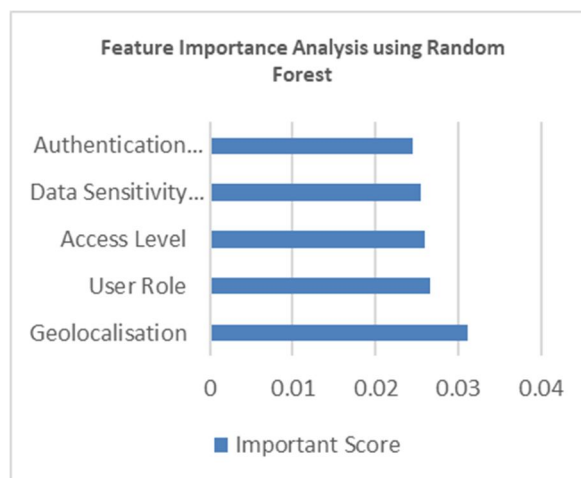


Figure 2: Feature Importance Analysis using Random Forests. Key features, such as geolocation restrictions and user roles, demonstrate greater importance for security resilience. Figure

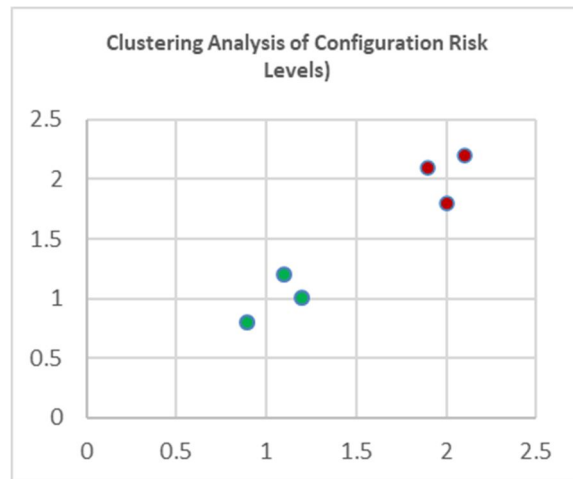


Figure 3: Clustering Analysis of Configuration Risk Levels. Clusters reveal that high-risk configurations often lack essential controls like MFA and dynamic access management

Risk Classification via Threshold: Using a threshold to classify configurations according to security scores revealed that 17.7% of configurations were high-risk, typically having single-layer authentication and limited control granularity.

D. Feature Analysis of High-Risk Configurations

An in-depth analysis of high-risk configurations highlighted common vulnerabilities associated with specific security features.

TABLE I: AVERAGE FEATURE VALUES IN HIGH-RISK CONFIGURATIONS

Geolocation Restrictions	Average Value (High-Risk)
Australia	3570
Germany	3524
India	3576
UK	3478
US	3507
User Roles	
Admin	4441
Guest	4374
Super Admin	4438
User	4402
Access Levels	
Modify	4359
Read	4473
Write	4366
Data Sensitivity Classification	
Confidential	4523
Highly Confidential	4300
Private	4357
Public	4475
Authentication Mechanisms	
Biometric	4349
MFA	4489
Password	4421
SSO	4396

Table 1 summarises the critical vulnerabilities associated with high-risk configurations, illustrating the need for enhanced geolocation restrictions, fine-grained access levels, and robust multi-factor authentication to mitigate security risks. Configurations with a Security Score above 3.80 are classified as Low-Risk, while those below this threshold are classified as High-Risk, as presented in Table 2.

V. DISCUSSION

The analysis of cloud security configurations highlights deficiencies in traditional security approaches, underscoring the need for adaptable, multi-layered security frameworks to address modern threats. Through descriptive statistics, correlation analysis, and machine learning, this study identifies critical limitations in conventional configurations and outlines opportunities for substantial improvement.

A. Key Insights and Analysis

Role of Geolocation Restrictions and User Roles: The feature importance analysis identified geolocation restrictions and user roles as significant determinants of higher security scores. This finding suggests that setting up location-based access restrictions and role-based permissions can significantly lower the chances of unauthorised access, ensure that access rights are appropriate for the situation, and improve safety in cloud-based settings where boundaries [10] [11]. **Limitations of Simple Access Control Models:** Clustering analysis shows that setups with many risks often have limited access control, especially when only role-based access control (RBAC) is used. Although RBAC is prevalent, its lack of adaptability to contextual factors limits its effectiveness. On the other hand, Attribute-Based Access Control (ABAC) offers an improved model by dynamically adjusting permissions based on user attributes and environmental variables, reducing vulnerabilities inherent to static access models [12].

Relevance of Multi-Factor Authentication (MFA): The threshold-based classification method underscores the higher risk associated with configurations relying solely on password authentication. Using multi-factor authentication (MFA) makes security much more robust by adding more layers of verification. It is a crucial defence against unauthorised access, especially when single-factor authentication leaves systems open to attack [13]. **Importance of Zero-Trust Architecture:** The study highlights the efficacy of Zero-Trust principles, particularly continuous session monitoring and verification, in cloud security [14]. Zero-Trust minimises insider threats and lateral movement risks by enforcing consistent verification for every access attempt, irrespective of user trust level [15]. The elevated security scores in configurations with Zero-Trust underscore its value in mitigating cloud vulnerabilities.

B. Practical Implications for Cloud Security

The findings offer actionable insights for strengthening cloud security strategies.

Adoption of Adaptive Security Controls: Static security methods are increasingly inadequate as cloud environments evolve. Because they can respond instantly to new threats, adaptive controls like ABAC and MFA circumvent the problems that come with traditional setups, strengthening security.

Implementation of Zero-Trust Principles: Adopting Zero-Trust Architecture mitigates external and internal security risks by requiring continuous access verification. This approach fortifies the security perimeter and minimises the potential for unauthorised lateral movement within networks [16].

Data Sensitivity Classification: Prioritising data based on sensitivity levels enables organisations to allocate security resources more effectively. Organisations can optimise security measures by applying heightened protections to high-value assets while maintaining efficient access controls [17].

These findings promote a deeper understanding of effective cloud security practices and provide strategic recommendations to enhance organisational resilience against modern security threats. They also advance the theoretical knowledge of cloud security vulnerabilities and provide actionable insights for practitioners implementing adaptive controls and Zero-Trust Architecture in cloud systems.

C. Future Research Directions

This work highlights the advantages of adaptive security and Zero-Trust principles; further studies may investigate using AI-driven anomaly detection to improve security protocols. Furthermore, comparing the efficacy of these methodologies across diverse cloud service providers and industries could offer a comprehensive view of cloud security policies and uncover sector-specific factors. By implementing the recommendations outlined in this study, businesses may substantially enhance their cloud security posture, reducing risks and establishing a safe foundation for their digital assets.

VI. CONCLUSION

This study comprehensively analyses vulnerabilities in cloud security configurations, identifying essential components for resilient frameworks. Through descriptive and machine-learning techniques, the research highlights critical security features such as geolocation restrictions, role-based access, and MFA. A multi-layered

approach incorporating MFA, ABAC, and Zero-Trust Architecture significantly enhances security. Additionally, data sensitivity classification enables efficient resource allocation to protect high-value assets. These insights contribute to academic research and practical strategies for cloud security, supporting the development of adaptable and resilient cloud systems.

A. Statements and Declarations

Conflicting Interest

The author(s) declared no potential conflicts of interest concerning this article's research, authorship, and publication.

Funding Statement

The authors did not receive support from any organisation for the submitted work.

Author Contribution

All the authors whose names appear on the submission contributed substantially to the conception or design of the work or the acquisition, analysis, and interpretation of data.

Data Availability Statement

This published article and its supplementary information files, which include all the data generated or analysed during this study, are available upon request from the corresponding author (kmf.mupila@gamil.com).

Declaration of AI-assisted technologies in the Writing process

The authors used generative AI for language editing and took full responsibility

REFERENCES

- [1] Cloud Security Alliance, "Cloud Security Alliance," 2024. [Online]. Available: <https://cloudsecurityalliance.org/research/topics/top-threats#>.
- [2] Google Cloud, "Google Cloud," Google, 16 October 2024. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023>.
- [3] S. Mehraj and M. T. Banday, "A flexible fine-grained dynamic access control approach for a cloud computing environment," *Cluster Computing*, vol. 24, pp. 1413-1434, 04 November 2020.
- [4] S. Mandal, D. A. Khan and S. Jain, "Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic," *New Generation Computing*, vol. 37, pp. 599-622, 29 June 2021.
- [5] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, 30 September 2024.
- [6] Thales, "Thales," 2024. [Online].
- [7] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye and T. O. Oladoyinbo, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, and Access Control within Cloud-Based Systems," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38-56, 25 January 2024.
- [8] S. A. Khan and S. M. I. Shamshuddin, "Access Control System Using AI and Blockchain," *International Journal for Multidisciplinary Research (IJFMR)*, vol. 6, no. 2, 2024.
- [9] W. Kandolo, "Ensuring AI Data Access Control in RDBMS: A Comprehensive Review," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2024.
- [10] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, pp. 422-450, 12 September 2023.
- [11] R. Yeluri and E. Castro-Leon, "Boundary Control in the Cloud: Geo-Tagging and Asset Tagging," in *Building the Infrastructure for Cloud Security*, Berkeley, Springer, 2014, pp. 93-121.
- [12] S. Ahmadi, "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *Journal of Information Security*, vol. 15, pp. 148-167, 6 May 2024.
- [13] M. Dawood, S. Tu, C. Xiao, H. Alasmay, M. Waqas and S. U. Rehman, "Cyberattacks and Security of Cloud Computing: A Complete Guideline," *Symmetry*, vol. 15, no. 11, p. 1981, 26 October 2023.
- [14] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K. U. Nisa and Y. Hamid, "A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model," *Sensors*, vol. 24, no. 4, p. 1328, 19 February 2024.
- [15] H. Kang, G. Liu, Q. Wang, L. Meng and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," *Entropy*, vol. 25, no. 12, p. 1595, 28 November 2023.
- [16] K. T. Santullo, "Case Study: Building a Zero Trust Architecture to Support an Enterprise," *ISACA Journal*, vol. 2021, no. 2, 26 February 2021.
- [17] Y. Zhang, H. Liu and G. Wang, "Data Sensitivity and Classification Management: A Declarative Approach," *International Journal of Information and Communication Sciences*, vol. 6, no. 3, 9 August 2021.