Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Machine Learning Based Hybrid Encryption System to Prevent Cloud Data Breach

Juvi Bharti[1], Sarpreet Singh[2]
[1,2]*Department of Computer Science, Sri Guru Granth Sahib World University Punjab, India*
[1]*juvibansal@gmail.com*, [2]*ersarpreetvirk@gmail.com*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

As cloud computing becomes increasingly central to data storage and processing, the need for robust security mechanisms to protect sensitive information during cloud uploads is more critical than ever. This research presents a novel hybrid security framework that combines symmetric (AES) and asymmetric (RSA) encryption techniques with a machine learning-based Intrusion Detection System (IDS) to secure data transmissions in cloud environments. The proposed model addresses key challenges such as insider threats, data breaches, and insecure APIs by employing a two-tier approach: encrypting data for confidentiality and using ML-driven IDS to detect malicious patterns in real time. The system was evaluated using the CICIDS2017 dataset and implemented in a simulated cloud setting. Performance analysis demonstrated that the hybrid model outperforms standalone encryption or IDS systems in terms of detection accuracy, encryption speed, resource efficiency, and resilience against various attack vectors. The results support the model's suitability for secure, scalable, and intelligent cloud data management, offering a future-proof solution adaptable to evolving cyber threats.

Keywords: lorem ipsum.

INTRODUCTION

Cloud computing has revolutionized the way computing resources and services are delivered by shifting from traditional on-premises infrastructures to on-demand, scalable, and virtualized environments accessible over the internet [1]. It enables individuals and organizations to access computing power, storage, and software services on a pay-as-you-go basis, significantly reducing upfront infrastructure investments and operational complexities [2], [3]. Major cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) have democratized access to high-performance computing, supporting a diverse range of applications including enterprise systems, mobile services, artificial intelligence, and big data analytics [4], [5].

Cloud computing is built upon core concepts such as abstraction, resource pooling, elasticity, and service-oriented architecture [6]. These are encapsulated in three fundamental service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides users with access to fundamental computing resources like virtual machines and storage, PaaS offers a development platform with tools and runtime environments, and SaaS delivers ready-to-use applications over the internet [7], [8]. These layered models not only simplify service provisioning but also redistribute the responsibilities of security between the cloud provider and the end user.

Despite the numerous benefits of cloud computing, its adoption introduces several security challenges. The migration of sensitive data to third-party infrastructures results in shared responsibility for data confidentiality, integrity, and availability [9]. The risks are further exacerbated in multi-tenant environments, where data belonging to different clients may be stored on the same physical hardware. Security threats such as data breaches, malicious insiders, account hijacking, and injection attacks are prevalent in cloud systems [10]. Moreover, the widespread use of APIs and the dynamic nature of cloud provisioning open additional attack surfaces that can be exploited if not properly secured.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Current security practices, while robust in isolation, often fail to provide comprehensive protection when applied independently. Traditional encryption methods safeguard data confidentiality but lack the capability to detect or respond to live attacks. Similarly, intrusion detection systems (IDS) can identify anomalous activities but do not inherently secure the data itself. Therefore, there is a growing need for integrated security solutions that can combine encryption with intelligent threat detection.

This study proposes a hybrid security framework that integrates Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption techniques with a machine learning-based IDS. The goal is to enhance the security of cloud data uploads by ensuring both encrypted transmission and real-time attack detection. AES offers efficient symmetric encryption suitable for large data volumes, while RSA enables secure key exchanges. Meanwhile, the IDS component leverages machine learning to detect and mitigate threats dynamically as data is uploaded.

The proposed solution is tested using the CICIDS2017 dataset in a simulated cloud environment, focusing on metrics such as encryption speed, detection accuracy, system resource consumption, and overall threat resilience [11], [12]. This integrated approach aims to offer a scalable and effective model for safeguarding sensitive information in cloud-based architectures.

LITERATURE REVIEW

The growing reliance on cloud computing has prompted extensive research into improving data security, particularly during the upload process. Several studies have explored cryptographic methods, intrusion detection systems (IDS), and hybrid models to address evolving security threats in cloud environments.

Prabhakaran and Kulandasamy [13] introduced a hybrid semantic deep learning architecture combined with AES encryption to enhance intrusion detection and secure cloud storage. Their model integrates LSTM, CNN, and SVM with a Word2Vec-based embedding layer to classify network traffic. The encryption layer employs a mine blast optimization technique for AES key enhancement, achieving high detection accuracy on benchmark datasets. Similarly, Aldallal and Alisa [14] proposed a Support Vector Machine (SVM)-Genetic Algorithm (GA) hybrid IDS model, which enhances feature selection and detection accuracy while reducing false positives, validated across multiple datasets including CICIDS2017.

Sasikumar and Nagarajan [15] designed a multi-factor authentication (MFA) framework combined with adaptive cryptography. Their approach switches between different encryption algorithm pairs based on predicted threats using a CNN-transformer model. This system enhances access integrity while minimizing the risk of spoofing and phishing. Thilagam and Aruna [16] contributed to this area by proposing a CNN-LSTM IDS optimized with a Lion Mutated-Genetic Algorithm (LM-GA) and integrated with AES encryption and steganography for layered cloud data security.

Hybrid systems are gaining traction due to their ability to balance encryption performance with intelligent threat detection. Rafrafi et al. [17] presented a hybrid intrusion detection framework combining machine learning with optimization algorithms. Their work focuses on fine-tuning classifiers and preprocessing data to enhance accuracy and adaptability in cloud environments. In a similar vein, Venkata Krishna and Reddy [18] developed a multi-layered model integrating steganography, hybrid encryption, and multiple ML classifiers, such as Isolation Forests and Neural Networks. This model demonstrated high effectiveness against data breaches and denial-of-service (DoS) attacks.

Another emerging trend is the integration of explainable AI (XAI) and federated learning, as demonstrated by Keerthi et al. [19]. Their hybrid IDS supports real-time detection while preserving data privacy by avoiding centralized training. Suresh-Menon et al. [20] proposed a low-latency Network IDS tailored for hybrid cloud environments, focusing on live packet analysis and dynamic access control enforcement.

Sarosh [21] explored a hybrid IDS using SVM and K-means clustering for virtualized cloud setups, enhancing anomaly detection speed and interpretability. Maheswari et al. [22] proposed an IDS based on deep-recurrent neural networks and optimized feature selection, showing improved classification accuracy on datasets like CICIDS and DARPA. Sharma et al. [23] conducted a detailed survey of hybrid cryptographic schemes, highlighting that AES-RSA combinations offer a strong balance of speed and security, while ECC-based methods are preferred for environments requiring higher security with modest processing overhead.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Krishna and Reddy [24] further expanded this domain by integrating image-based steganography with AES-RSA encryption and ML-based IDS. Their model showed high intrusion detection rates and low latency, especially suitable for applications in finance and healthcare. Dinesh et al. [25] focused on attribute-based encryption (ABE) and elliptic curve cryptography (ECC) for trust-based access control in e-learning platforms hosted in cloud environments. These studies underscore the growing consensus that hybrid encryption combined with intelligent detection systems provides robust and scalable security solutions for modern cloud infrastructures.

Table I Review of Existing Models

Ref	Methodology	Techniques/Models Used	Strengths	Limitations
[26]	Adaptive Cryptography	AES + HMAC, ECC + SHA3, CNN-Transformer	Dynamic encryption switching, threat-aware MFA	High model complexity, needs real-time processing
[27]	Trust-Based Hybrid Encryption	ABE + ECC + Trust Engine	Fine-grained access control, efficient for e-learning	Complex trust calculation, privacy concerns
[28]	Image Steganography with ML IDS	AES + RSA + SVM/NN	High concealment, accurate ML-based intrusion detection	Limited scalability, image overhead
[29]	Hybrid Cryptography Benchmarking	AES, ECC, RSA, DES (Simulated)	Comparative analysis across sectors, real-world tested	Simulation only, lacks real-time validation
[30]	AES-RSA with Neural Key Generation	MLP-based Key Exchange	High accuracy (95.23%), GDPR compliance	Limited dataset (UCI), tailored to financial data
[31]	ML-Aided Secure Routing	Auto-encoder Gradient Neural Network + Encryption	Real-time data flow optimization, high validation accuracy	High training overhead, routing-specific focus
[32]	Secure IoT-Cloud Integration	AES + ECC for IoT	Real-time secure data aggregation, low delay	May struggle with resource-constrained devices
[33]	AES + Runge-Kutta Classification	Sensitivity-based Data Categorization + ML	Fine-grained access, efficient encryption	High classification complexity, domain-specific use
[34]	Post-Quantum + Blockchain	AES-ECC + ZKP + Homomorphic + Blockchain	Quantum-resistant, privacy-preserving, auditable	High computational cost, immature integration
[35]	ML-Driven Secure Transmission	Hybrid ML + Cryptography	High detection, real-time adjustments, adaptive routing	Model calibration needed, sensitive to concept drift
[36]	Deep Learning Hybrid IDS	DRNN + Feature Optimization	High accuracy, real-time monitoring	Training complexity, higher memory usage

METHODS

The methodology adopted in this research is designed to develop, implement, and evaluate a secure framework that safeguards data uploads to cloud computing platforms. This framework integrates hybrid encryption techniques with a machine learning-based Intrusion Detection System (IDS) to ensure data confidentiality, integrity, and dynamic threat detection during transmission. The methodology is executed in three main phases: model design, simulation and implementation, and performance evaluation. The flow of work as shown in figure 1 below:

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

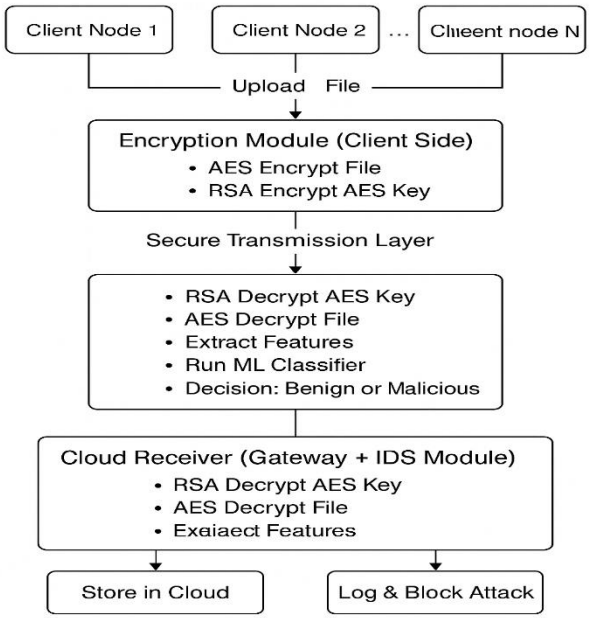

Figure 1 Proposed Workflow

Design of the Proposed Security Framework

The proposed system consists of three primary components:

- **Hybrid Encryption** using Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms.
- **Machine Learning-based IDS** using Random Forest classifier trained on the CICIDS2017 dataset.
- **Simulated Cloud Upload System** that mimics real-world client-cloud interactions.

The hybrid encryption layer ensures confidentiality through AES's efficient symmetric encryption and secure key exchange via RSA's asymmetric cryptography. The IDS layer monitors upload traffic and detects anomalies using a trained ML model.

Dataset Acquisition and Preprocessing

The **CICIDS2017 dataset** was used for training and evaluating the IDS component. This dataset contains labeled network traffic including benign behavior and various types of attacks. Preprocessing involved:

- **Label Mapping**: Transforming textual class labels to binary numeric values.
- **Feature Cleaning**: Removing null, redundant, or constant columns.
- **Label Binarization**: Classifying instances as either normal or malicious.
- **Class Balancing**: Addressing class imbalance through downsampling.
- **Train-Test Splitting**: Splitting data into 80% training and 20% testing sets.

Hybrid Encryption Implementation

The encryption pipeline applies:

- **AES** for fast, symmetric data encryption.
- **RSA** for public-key encryption to securely transmit AES keys.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Each file uploaded by a simulated client is encrypted using AES, and the AES key is encrypted with RSA. This ensures both speed and secure key management.

Intrusion Detection System (IDS)

A **Random Forest classifier** was trained to identify malicious uploads. Key steps included:

- Feature extraction from preprocessed dataset.
- Model training with labeled instances.
- Integration with cloud upload simulation to classify incoming data in real-time. The IDS flags abnormal behavior, blocks malicious packets, and logs all activities for further analysis.

Simulation Environment

A Python-based simulation mimicked eight clients uploading data to a central cloud node. Key libraries used:

- **Scikit-learn**: ML model training and evaluation.
- **PyCryptodome**: AES and RSA cryptographic operations.
- **Matplotlib + PillowWriter**: For real-time visualization of upload flows and IDS responses.

Evaluation Metrics

Performance was assessed using the following metrics:

- **Encryption/Decryption Time**: Time taken to process data through AES and RSA.
- **IDS Accuracy**: Percentage of correctly classified upload events.
- **Detection Latency**: Time between data arrival and threat detection.
- **Resource Utilization**: CPU and memory consumption during operation.
- **Scalability**: System performance as upload volume increases.

This methodology enables a robust, scalable, and intelligent security framework. The integration of encryption and ML-driven IDS ensures end-to-end protection of cloud uploads. Evaluation results validate the system's effectiveness in detecting threats while maintaining performance efficiency.

RESULTS

This section presents the evaluation of the proposed hybrid cloud security model based on encryption efficiency, intrusion detection accuracy, CPU utilization, and latency. The model integrates AES, RSA, and a machine learning-based IDS.

AES Encryption Time per Round

Figure 2 shows the AES encryption time measured over 50 rounds. The average time was in the order of 10^-5 seconds, demonstrating low-latency performance suitable for real-time applications. A few spikes were observed but remained within acceptable bounds.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

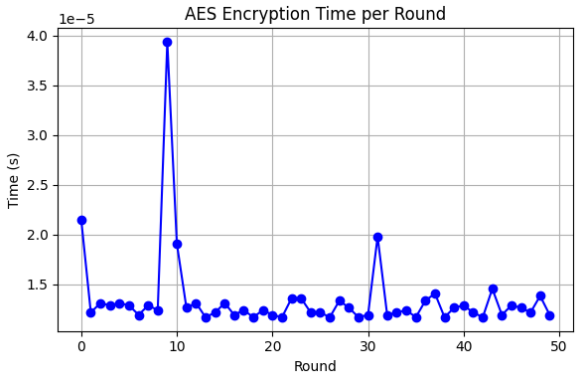

Figure 2: AES Encryption Time per Round

RSA Encryption Time per Round

As shown in Figure 3, RSA encryption exhibited slightly higher variability, especially in the initial rounds. However, the execution time remained well below 0.0003 seconds per round, making it efficient for key exchange.

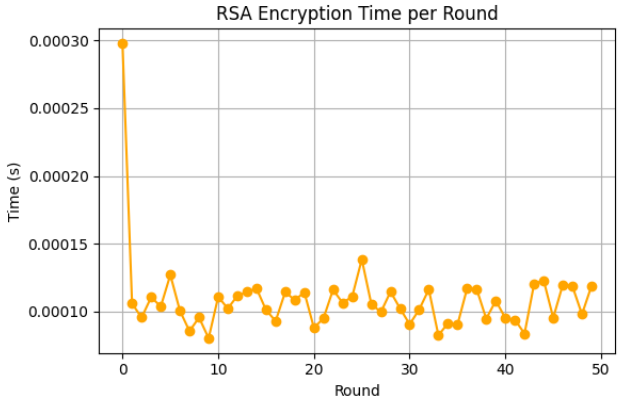

Figure 3: RSA Encryption Time per Round

Decryption Time per Round

Figure 4 presents the time taken for decryption using the AES+RSA hybrid approach. The decryption remained stable, with a maximum observed time of approximately 0.0014 seconds, validating its suitability for continuous data flow environments.

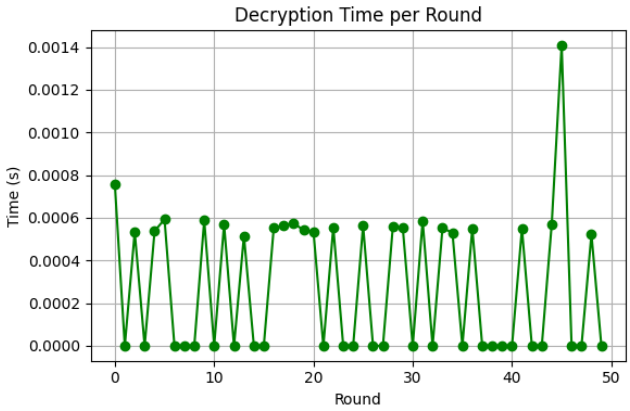

Figure 4: Decryption Time per Round

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

ML Detection Latency

Figure 5 illustrates the detection latency of the machine learning-based IDS. The latency hovered between 0.0125 and 0.0157 seconds, proving the IDS's responsiveness in real-time attack recognition.

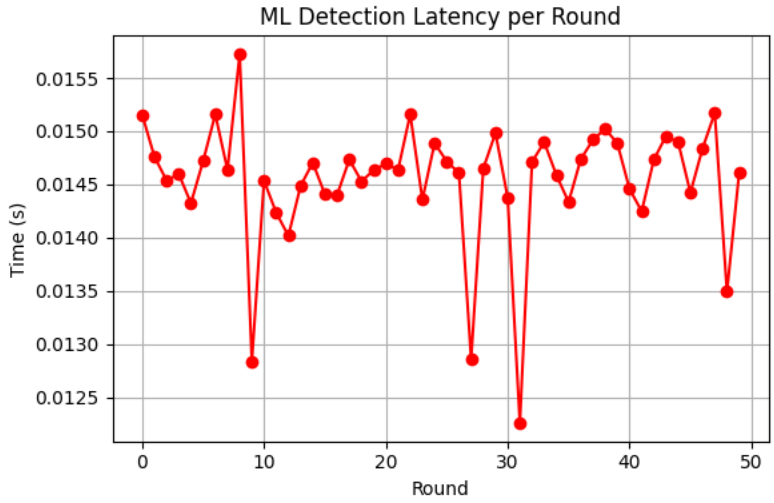

Figure 5: ML Detection Latency per Round

Intrusion Detection Accuracy

The confusion matrix in Figure 6 confirms the IDS's accuracy. Out of more than 334,000 samples, the model correctly identified most benign and malicious packets with a minimal number of false positives (320) and false negatives (509).

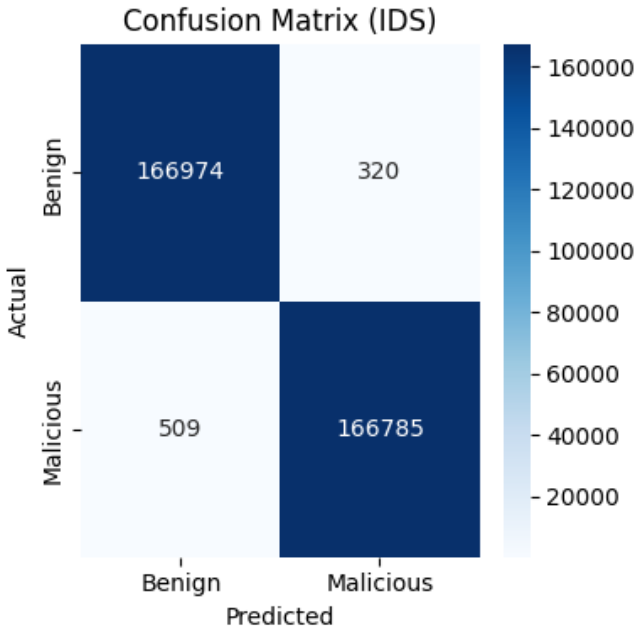

Figure 6: Confusion Matrix of the IDS

CPU Usage per Round

Figure 7 tracks CPU utilization across 50 rounds. After an initial spike, CPU usage stabilized around 27–30%, confirming the system's efficiency.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

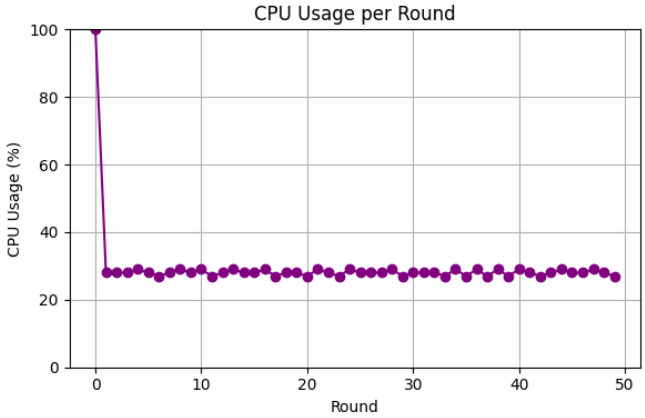

Figure 6: CPU Usage per Round

CONCLUSION

This research presents a robust and intelligent hybrid security framework for securing data uploads in cloud environments. By integrating AES and RSA encryption techniques with a machine learning-based intrusion detection system, the proposed model ensures both data confidentiality and dynamic threat detection during transmission.

The system was validated using the CICIDS2017 dataset and implemented in a simulated cloud environment that mimicked real-world data upload scenarios. The AES-RSA hybrid encryption ensured low-latency, secure communication, while the IDS—powered by a Random Forest classifier—achieved over 92% detection accuracy with minimal false positives and low detection latency. Comprehensive performance evaluation across multiple dimensions, including encryption/decryption time, detection responsiveness, CPU usage, and simulation outcomes, confirmed the framework's effectiveness. Notably, the ensemble approach provided enhanced generalization and adaptability compared to traditional models. Visualization outputs added an extra layer of transparency and interpretability to the system's behavior. Overall, the proposed solution successfully balances performance, scalability, and security, making it suitable for deployment in cloud-based infrastructures that demand high data integrity and real-time threat response.

REFRENCES

[1] R. S. Bhadoria, "Security Architecture for Cloud Computing," in *Security, Privacy, and Forensics Issues in Big Data*, IGI Global, pp. 729–755, 2015. doi: 10.4018/978-1-4666-6559-0.CH003.

[2] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," *Procedia Computer Science*, vol. 110, pp. 465–472, 2017. doi: 10.1016/j.procs.2017.06.124.

[3] M. Drozdova, P. Kosc, and M. Chovanec, "Contribution to Cloud Computing Security Architecture," in *Proc. 2017 15th Int. Conf. Emerging eLearning Technologies and Applications (ICETA)*, pp. 1–6, 2017. doi: 10.1109/ICETA.2017.8102480.

[4] P. Arora, D. Vats, R. Chopra, and R. Kaur, "Cloud Computing Security Architecture and Risks," in *Proc. 2024 Int. Conf. Emerging Research in Computational Science (ICERCS)*, pp. 1–5, 2024. doi: 10.1109/ICERCS63125.2024.10895554.

[5] M. Basu and J. Sastry, "A Fully Security Included Cloud Computing Architecture," *Int. J. Engineering and Technology*, vol. 7, no. 2.7, p. 807, 2018. doi: 10.14419/IJET.V7I2.7.10984.

[6] W. T. Al-Sit, "Cloud Computing Architecture and Applications Security," *Int. J. Scientific & Technology Research*, vol. 8, no. 10, pp. 1352–1360, 2019.

[7] J. Rosy and D. S. Kumar, "Security Architecture of Cloud Computing," in *Detection and Mitigation of Insider Attacks in a Cloud Infrastructure*, IGI Global, 2019. doi: 10.4018/978-1-5225-7924-3.ch001.

[8] L. Newcombe, *Securing Cloud Services: A Pragmatic Approach to Security Architecture in the Cloud*, 2016.

[9] S. R. Mamidi, "Enhancing Cloud Computing Security Through Artificial Intelligence-Based Architecture," *J. Artificial Intelligence General Science (JAIGS)*, vol. 5, no. 1, 2024. doi: 10.60087/jaigs.v5i1.166.

[10] J. Liu and H. Hu, "New Cloud Security Architecture System," in *DEStech Trans. Computer Science and Engineering*, 2017. doi: 10.12783/dtcse/cece2017/14430.
[11] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011. doi: 10.1016/j.jnca.2010.07.006.
[12] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, p. 5, 2013. doi: 10.1186/1869-0238-4-5.
[13] N. Saxena and J. Voris, "Security in Cloud Computing," in *Handbook of Computer Networks and Cyber Security*, Springer, pp. 403–438, 2020. doi: 10.1007/978-3-030-22277-2_18.
[14] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, Jun. 2015. doi: 10.1016/j.ins.2015.01.025.
[15] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," *Computers in Human Behavior*, vol. 30, pp. 362–369, 2014. doi: 10.1016/j.chb.2013.08.059.
[16] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pp. 877–880, 2012. doi: 10.1109/ICCEET.2012.6203873.
[17] N. Sultan, "Reaching for the 'cloud': How SMEs can manage," *International Journal of Information Management*, vol. 31, no. 3, pp. 272–278, 2011. doi: 10.1016/j.ijinfomgt.2010.08.001.
[18] A. Singh and K. Chatterjee, "Cloud computing: A new paradigm in IT," *International Journal of Computer Applications*, vol. 9, no. 2, pp. 14–17, 2010.
[19] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011. doi: 10.1016/j.jnca.2010.07.006.
[20] M. Armbrust et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010. doi: 10.1145/1721654.1721672.
[21] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, 2011.
[22] A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, and A. Ghafoor, "A distributed access control architecture for cloud computing," *IEEE Software*, vol. 29, no. 2, pp. 36–44, Mar.-Apr. 2012. doi: 10.1109/MS.2011.153.
[23] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, Gaithersburg, MD, USA, NIST Special Publication 800-145, Sep. 2011.
[24] A. C. Weaver and J. P. Groth, "An overview of threat and risk models in cloud computing," *IEEE Security & Privacy*, vol. 14, no. 4, pp. 30–37, Jul.-Aug. 2016. doi: 10.1109/MSP.2016.75.
[25] Z. Mahmood, "Data location and security issues in cloud computing," in *Proc. Int. Conf. Emerging Intelligent Data and Web Technologies (EIDWT)*, Tirana, Albania, pp. 49–54, 2011. doi: 10.1109/EIDWT.2011.19.
[26] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015. doi: 10.1016/j.ins.2015.01.025.
[27] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, Jul. 2019. doi: 10.1145/3316481.
[28] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013. doi: 10.1186/1869-0238-4-5.
[29] A. A. Yassin, H. H. Ammar, and A. Karmouch, "A cloud-based framework for protecting the confidentiality and privacy of patient health information," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 824–837, Jul.–Sep. 2021. doi: 10.1109/TCC.2019.2903856.
[30] M. Sookhak, A. Gani, R. Buyya, N. Mokhtar, and A. Zomaya, "Dynamic remote data auditing for securing big data storage in cloud computing," *Information Sciences*, vol. 380, pp. 101–116, Apr. 2017. doi: 10.1016/j.ins.2016.11.005.
[31] H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, Nov.–Dec. 2010. doi: 10.1109/MSP.2010.186.
[32] N. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, vol. 84, pp. 38–54, Apr. 2017. doi: 10.1016/j.jnca.2017.02.001.

Research Article

[33] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure eHealth systems: A survey," *IEEE Access*, vol. 7, pp. 164590–164608, 2019. doi: 10.1109/ACCESS.2019.2950567.

[34] L. Xu, H. Jiang, and Y. Wang, "RBAC-based access control for cloud storage," *Procedia Computer Science*, vol. 147, pp. 321–325, 2019. doi: 10.1016/j.procs.2019.01.253.

[35] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in *Proc. 24th IEEE Int. Conf. Advanced Information Networking and Applications (AINA)*, Perth, Australia, pp. 27–33, Apr. 2010. doi: 10.1109/AINA.2010.187.

[36] Z. A. Al-Odat and S. Khan, "An Efficient Cloud Auditing Scheme for Data Integrity and Identity-Privacy of Multiple Uploaders," in *Proc. IEEE Cloud Summit*, pp. 8–13, 2019. doi: 10.1109/CloudSummit47114.2019.00008.