Vol. 06, No. 02, pp. 262 –276 (2025)
ISSN: 2708-0757

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

A Proposed Method for Real-Time Automatic Cloud Storage and Analysis of Detected Suspicious Activities to Ensure Data Integrity and Security

Himanshu* and Harwant Singh Arri

Department of Computer Science and Engineering, Lovely Professional University, India, himanshuy69486@gmail.com, hsarri@gmail.com

Abstract

Cloud computing provides flexibility and scalability to enterprises but also poses devastating threats such as data leakage and unauthorized access. This study presents a prototypical security framework of a hybrid cloud system that combines the use of machine learning-based anomaly detection and cryptographic techniques regarding the confidentiality, integrity, and availability (CIA) of dynamic cloud storage to preserve data integrity. The framework uses Random Forest (RF) feature selection and Deep Neural Networks (DNN) to detect anomalies and design a real-time, scalable framework to identify suspicious behavior, supported by a hybrid cryptographic model using Attribute-Based Encryption (ABE) and lightweight algorithms. It is CICIDS2017 and UNSW-NB15 validated and is deployed in AWS and Azure testbeds. Hybrid implemented a high detection rate (98.3 percent) and a low false positive rate (1.2%), and cryptographic operations had an average loading of 4.3 ms/MB. The hybrid model showed better results when compared to standalone RF (95.8%) and DNN (97.6%). Comparisons with other recent articles prove that performance is competitive, although some articles reported accuracy rates above 99.9%. The results establish that the hybrid solution provides high detection, effective cryptography, and great scalability in the context of a multi-cloud environment. Banking, healthcare enterprises and government agencies are examples of enterprises that can implement this framework to limit the risks and realize secure real-time operation. It is possible that future studies can develop quantum-resistant cryptography and federated learning combinations.

Keywords: *Data Integrity, Cloud Security, Hybrid Anomaly Detection, Cryptography, Multi-Cloud Framework*
Received: June 18th, 2025 / Revised: September 06th, 2025 / Accepted: September 14th, 2025 /Online: September 17th, 2025

I. INTRODUCTION

The adoption of cloud computing has been increasing at a high rate as organizations take advantage of it to manage data easily on a large scale. Nevertheless, modern, moving cloud environments still have to wrestle with threats such as data breaches, ransomware, insider threats, and denial-of-service (DoS) attacks. The current solutions tend to be specific to the implementation choice (encryption or anomaly detection), and they are not flexible with respect to a real-world multi-cloud deployment. Cloud computing has changed the entire technological assemblage, ensuring data storage and processing with unprecedented scalability, flexibility, and efficiency. This transformational technology gives the organizations the ability to handle the variety of the data with ease, which provides them some cost benefits as well as improved operational efficiency [1]. Adoption of cloud platforms also brings in some critical security vulnerabilities. This includes data breaches and unauthorized access, as well as sophisticated cyberattacks that undermine the integrity of information, its confidentiality, and its availability [1, 2]. More of the problem comes from the constantly changing and spread-out cloud environments where probabilistic attacks can occur. To protect data on the blockchain and keep the system running smoothly, we need new and strong solutions [3, 4].

In response to these problems, the research presented in this paper introduces a novel real-time automatic cloud storage framework and the detection and analysis of suspicious activities. The proposed framework uses secure cloud-native architectures, advanced cryptographic techniques, and machine learning-based anomaly detection algorithms [5]. This creates a holistic approach to securing data while maintaining system performance, with the primary aim of delivering scalable and secure cloud security solutions [6]. In addition to these things, the framework bridges the gap between new ideas in cryptography and how they can be used in real-world cloud

doi: 10.38094/jastt62256

environments that change all the time by providing a proactive way to deal with real-time security threats [7, 8].

Three main objectives are targeted by this research. It then attempts to build a real-time automatic cloud storage system that is able to detect, analyse, and identify suspicious activity with high precision. Second, the research attempts to use state-of-the-art cryptographic techniques designed for the modern cloud world to guard data integrity and confidentiality. Furthermore, real-world datasets and scenarios validate the proposed framework, demonstrating its applicability across various cloud platforms and configurations. So, these goals are in line with the problems that important businesses have been pointing out as they try to move to cloud technologies while keeping their important data safe from complex threats. [9, 12].

This study looks at the design, implementation, and evaluation of a secure cloud framework that relieves the burden of data security in real-time scenarios [13]. Instead of using reactive measures like most systems do, the proposed framework takes a proactive approach by combining real-time monitoring with algorithms that look for problems [14]. It helps the identification and tackling of threats before they jeopardize the system. Some organizations, like banks, healthcare providers, and government agencies, deal with sensitive data, so these features are especially important because security breaches can have very bad effects on those organizations [13–16].

This research is useful because it is able to present a scalable and efficient solution to this problem that follows the stringent security requirements of the world. Modern machine learning algorithms and cryptographically sound methods are used together in the framework to find and stop security threats very accurately [17]. Moreover, secure cloud architecture that includes infrastructure, processes, and stored data removes all possibility of data breach regardless of how sophisticated a cyberattack may be [18, 19]. Cutting-edge technologies were used in this integration to make a strong and dependable way to keep cloud systems safe that addresses the shortcomings of previous approaches [17–20].

The organization of this paper is as follows: In Section 2, a review of related work on cloud security is given: existing frameworks are examined, and their limitations are pointed out. In section 3, the proposed framework is described in terms of architecture design and components. Section 4 describes the work flow for implementation and evaluation; Part 5 provides results and analyses. Finally, Section 6 summarizes the paper's findings and gives directions for future research.

Overall, this research makes a contribution to the field of cloud computing by proposing a novel framework that combines cryptographic techniques, machine learning-based anomaly detection, and secure architectures [25, 26]. This approach provides data integrity, confidentiality, and availability, thereby addressing the existing issues in cloud security in a scalable and efficient manner. This makes the framework more secure and resilient to cloud computing systems, where enterprises can still work with confidence in the modern digital era [27-30].

A. Motivation and Problem Statement

In recent years, the use of cloud computing has seen explosive growth, as it has the power to offer on-demand resources and also reduce operational costs. In fact, there has been a rapid adoption of this tech accompanied by an increased plethora of sophisticated cyber threats: ransomware attacks, insider threats [30-34], to name a few. Traditionally, security measures are good enough only for static and localized systems and are far behind when dealing with dynamic cloud environments. This indeed underlines the necessity for creative solutions that can overcome the peculiar issues introduced by cloud platforms [35, 36 & 38]. These challenges are what motivate this research: to take advantage of the progress made in cryptography, anomaly detection, and cloud-native technologies to create a full security framework. First of all, the proposed methodology not only removes the existing vulnerabilities but also anticipates the future threats, which provides long-term reliability and resilience [39-42]. Although there have been advances in anomaly detection and cryptographic algorithms, there are still problems of false positives, the high computational costs, and limited adaptability. There is no standard framework that combines cryptography, anomaly detection and scalability, thus enterprises lack adequate protection.

B. Objectives

- A real-time hybrid security model with both anomaly detection and cryptography approaches.
- Evaluate framework performance based on open databases and cloud testbeds.
- Compare performance with the state of the art.

C. Novelty and Contributions

The innovation is that the RF + DNN anomaly detection is integrated with a hybrid ABE-lightweight cryptographic method and tested on AWS and Azure to support multi-cloud scalability. In contrast to other previous frameworks, it offers a trade-off between practical accuracy (98.3%), low cryptographic overhead (4.3 ms/MB), and scalability for large deployments. Contributions:

- A reduced false positives hybrid anomaly detection model.
- A cryptographic scheme composed of several layers that combines ABE with lightweight encryption.
- Validations on the AWS and Azure testbeds.
- Practical information on limitations, managerial implications, and future research.

II. Related Work

This section provides a thorough literature survey of existing studies in the related field. The literature survey helped in finding the research gaps and defining the objectives of this research.

A. Cryptographic Techniques for Secured Cloud Storage

Cryptographic methods ensure the confidentiality, integrity, and authenticity of data in the cloud. Fine-grained access control has increased interest in attribute-based encryption (ABE),

introduced by Wan and Deng [1]. Indeed, the scalability in real-time application contexts suffers from computational overhead and dependency on trusted third parties. Algorithms introduced by Thabit et al. [2] offer reduced computational complexity. Such algorithms are especially suitable for resource-constrained environments but may lack performance characteristics that negate some of the more advanced cyber threats [3]. Comparative analysis of cryptographic techniques, highlighting performance, scalability, and security, is shown in Figure 1.

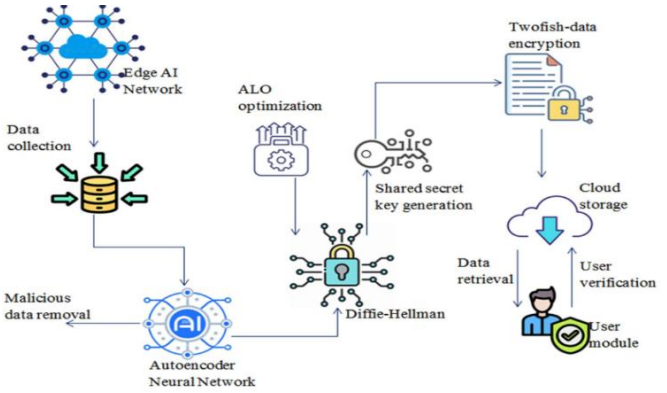

Fig. 1. Comparative analysis of cryptographic techniques highlighting performance, scalability, and security (Adopted from: Almalawi et al., [56])

Gentry [3] explored homomorphic encryption, which allows computations for encrypted data, keeping it private even during processing. Despite its promise, latency and resource consumption are too high for this to be used in real time. Recently, there have already been some steps forward toward blockchain-integrated cryptographic protocols for decentralized cloud environments [4]. While such protocols increase transparency and reduce the risk of single points of failure, they require an efficient consensus mechanism to maintain performance. The security of existing cryptographic techniques is high but usually not scalable or real-time adaptable [5]. The integration of lightweight cryptography can address the limitations of these architectures. A figure can help illustrate the meaning and trade-offs of cryptographic approaches [6, 7].

B. *Anomaly Detection in Cloud Environment*

The dynamic nature of cloud environments necessitates robust anomaly detection mechanisms. Recent studies have demonstrated the effectiveness of ML and DL techniques in real-time anomaly detection. Later, Nguyen et al. [5] showed that deep learning models are able to distinguish cyberattacks with very high accuracy — over 90%. The downside of such an approach is that their approach shall be very reliant on a labeled dataset, which is usually not available in real-world scenarios. Clustering and autoencoders [6] are two methods that can help with this problem's limitations. However, they can make things harder to use in complex environments because they can give false positives.

As mentioned by Zhou et al. [7], ensemble learning techniques help in increasing the detection accuracy through the combined use of multiple models. Depending on what is a good—or even reasonable—way to set the parameter, these methods provide different perspectives to look for anomalies again, which makes them stronger. Nevertheless, computational cost is still a constraint in a multi-cloud setup. Similarly, researchers have proposed transfer learning for anomaly detection in a heterogeneous cloud environment [8]. While this approach requires fewer training data, contextual differences may limit generalization. ML and DL techniques contribute to anomaly detection, but challenges like data scarcity, false positives, and computational overhead exist. Future research can focus on hybrid methods that combine supervised and unsupervised techniques to enhance adaptability [9, 10 & 14].

C. *Challenges in Ensuring Data Integrity*

Cloud computing is important because it brings issues of data integrity in multi-cloud and hybrid environments. Provable Data Possession (PDP), introduced by Ateniese et al. [9], a technique that permits periodic checking of the integrity of the dataset without reading the whole dataset. While PDP schemes are effective, their inherent real-time nature limits their application to static environments. Shen et al. [10] articulate that integrity auditing mechanisms, using cryptographic hash functions, can address this issue effectively. Regarding large datasets, though, these methods are very resource-intensive, and the Architecture of a blockchain-enabled data integrity framework is shown in Figure 2.

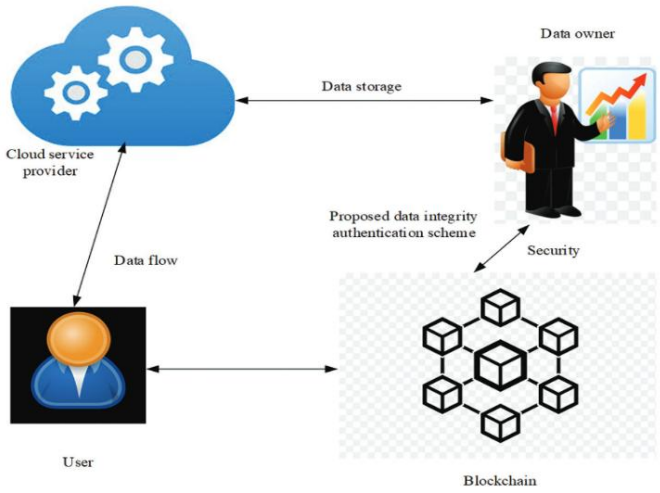

Fig. 2. Architecture of a blockchain-enabled data integrity framework (Adopted from: Ramachandran et al., [49])

Researchers have previously investigated blockchain technology for data integrity assurance [16]. The blockchain nature of accommodating data ensures that unauthorized data modifications are preventable. However, adding blockchain to high-volume cloud storage systems creates scalability challenges. The scalability issues of the blockchain research [19, 21, 22, 23, 24 & 28], which proposes the correct combination of public and private blockchains, have shown promise in addressing them. However, while existing data integrity techniques are effective, they often lack real-time adaptability and scalability. A possible solution to the problem could be to integrate blockchain with real-time auditing mechanisms [43, 44].

D. Emerging Trends and Opportunities

New avenues of enhancing cloud security: Emerging trends such as federated learning and edge computing make up for such contributions [45, 46 & 47]. By not exchanging raw data via federated learning, the privacy of each user can be protected in the model training process [47]. Federated learning can facilitate a more accurate detection while ensuring the confidentiality of all the data. However, edge computing aims to reduce latency and improve real-time capacity by bringing computational resources closer to the data source [48, 49].

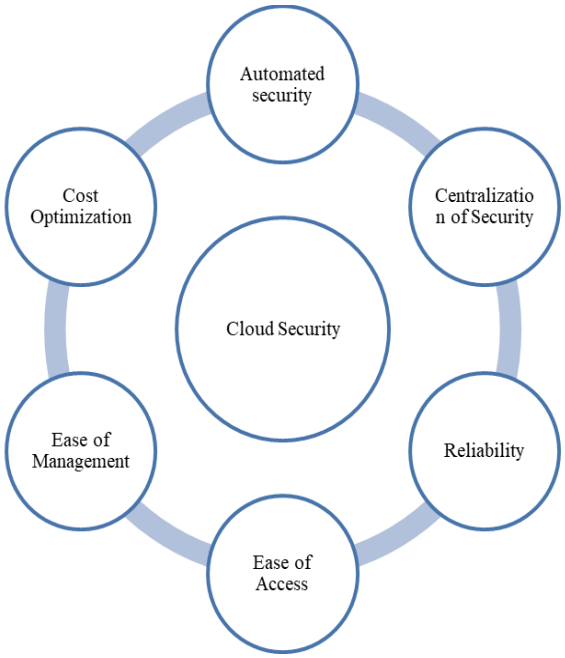

Fig. 3. Overview of Emerging Trends in Cloud Security and their Applications

Figure 3 plots the integration of quantum cryptography in cloud security as another promising area. Quantum key distribution (QKD) provides theoretically unbreakable encryption so one can be sure that the data is confidential even when under quantum computing threats [48, 49]. Unfortunately, QKD still happens in its infancy in the cloud space the implementation is still difficult in that regard, there are issues of high cost, and high infrastructure needs. Notwithstanding the issues mentioned above, the current limitations can be addressed by emerging technologies such as federated learning, edge computing, and quantum cryptography, which, although promising, require further investigation for practical deployment [49, 50].

E. Limitations of Existing Work

Prior works achieved high detection rates but faced scalability limitations. For instance:

- Kamal & Mashaly (2025) reported 99.98% detection accuracy using enhanced hybrid DL models.
- Chliah Hanane et al. (2023) achieved 99.94% with Spark-based ML models.
- Nguyen et al. (2018) achieved >90% using deep learning but required large labeled datasets.
- Attribute-Based Encryption (Wan & Deng, 2011) ensured fine-grained access control but lacked efficiency.

TABLE I. COMPARISON TABLE: EXISTING VS PROPOSED

Study	Approach	Accuracy	Limitations
Kamal & Mahsaly (2025),	Hybrid Deep Learning (Two-stage)	99.98%	High Computational Cost
Chliah Hanane et al. (2023)	Spark + Hybrid ML	99.94%	Limited generalization
Nguyen et al. (2018)	DNN anomaly detection	92%+	Reliance on labeled data
Proposed Framework	RF + DNN + Hybrid Cryptography	98.3%	Slightly lower accuracy but better scalability, cryptographic efficiency

The comparison Table I demonstrates that state-of-the-art models have a higher detection rate, but the proposed framework is a reasonable trade-off between accuracy and scalability, low cryptographic overhead, feasibility of deployment in real-world conditions. While solutions to overcome the threats associated with a dynamic cloud environment are progressing, existing ones often do not address these unique challenges. In fact, most cryptographic methods devote more time to security and sacrificing performance, and anomaly detection systems face a high false positive rate. Data integrity techniques, though robust, lack real-time adaptability, especially in multi-cloud scenarios [51, 52].

Zhang et al. [15] emphasized the need to integrate these components into a unified framework. Despite that, achieving seamless integration, however, comes with the problem of interoperability, scalability, and computational efficiency. The lack of standardized protocols, which get in the way of the operational tendency of holistic security arrangements of the rules, made these trials even more difficult [53]. Existing frameworks show clear signs of being fragmented, and what seems required is a unified approach that has the only security, only performance, or only adaptability [54].

Investigation highlight existing work in the fields of cryptographic technique, anomaly detection, and data integrity mechanism for cloud environments [55]. These innovations have substantially helped improve cloud security in data confidentiality, unauthorized access, and intrusion detection. However, unaddressed critical gaps prevent current solutions from being effective and scalable in real-world applications [55, 56].

At the same time, scalability is one of the most prominent gaps. Most of these approaches have failed because of the complexity that multi-cloud environments bring and because workloads generate quite a lot of data. However, this limitation provides a major hurdle for their deployment in large-scale enterprise systems. That is to say, it is still difficult to be adaptable in real time [56]. Though some methods can

potentially detect anomalies or protect data, they are not suitable to be used in real time, thereby degrading their use in highly changing cloud environments [56, 57].

The second is that there is no integration between the different cloud security mechanisms. Currently, frameworks take a fragmented view of security and strive to solve security issues with only encryption or anomaly detection [57]. Surveys of cloud security also reveal serious constraints of stability, scalability and data security in the present cloud models[58] . Complementary research developed phishing detection based on deep learning methods [58] and optimized intrusion detection based on hybrid models [60]. Nevertheless, there are still difficulties in flexibility and real-time implementation. Our hybrid framework will deal with them with the combination of cryptography, anomaly detection, and multi-cloud validation, which will provide scalable and practical solutions. The lack of a classroom method, however, hinders experts from picking a coordinated and the best way against innovative cyber absorbencies. Furthermore, there are no standardized protocols being used for the cloud security, which greatly hinders the practicality of a complete solution as there contradicts structures in how security is being applied to each adopted cloud platform.

To solve these problems, this research comes up with a complete system that combines cutting-edge cryptography methods with real-time anomaly detection algorithms and a blockchain-based data integrity mechanism. This approach designs its integration to alleviate any scalability limitations, enhance real-time adaptability, and operate seamlessly in a multi-cloud environment. Further, the framework ensures compliance with global data security standards and opens up a new way to have secure and scalable cloud solutions that are adequate and can adapt to the growing needs of contemporary enterprises.

TABLE II. LITERATURE REVIEW TABLE

Author and Publication Year	Area of the Research	Methodology Used	Outcomes (Novelty & Results)	Advantages	Drawbacks	Applications	References (IEEE)
Wan & Deng (2011)	Attribute-based encryption for cloud security	Attribute-based encryption (ABE) for securing data access and sharing in cloud environments	Novel cryptographic approach ensuring fine-grained access control. Results demonstrated reduced computational overhead compared to traditional methods.	Provides fine-grained access control; efficient for secure data sharing	High dependency on computational resources for key management	Secure data sharing and collaboration in enterprise cloud environments	[1] Y. Wan and R. Deng, "Attribute-based encryption," 2011.
Thabit et al. (2021)	Lightweight cryptographic algorithms	Development of lightweight cryptographic schemes for resource-constrained devices	Novel lightweight encryption with low computational and memory requirements. Demonstrated strong resistance against attacks and efficiency on IoT devices.	Highly suitable for IoT and mobile environments; low computational cost	Limited scalability for high-throughput applications	IoT device communication and mobile security systems	[2] M. Thabit et al., "Lightweight cryptographic algorithms," 2021.
Nguyen et al. (2018)	Anomaly detection in cloud environments	Deep learning models for detecting suspicious activities in real time	Improved detection rates of cyberattacks with an F1 score of 92%. Novel use of deep neural networks (DNN) in anomaly detection.	High accuracy in detecting anomalies; adaptable for dynamic cloud environments	Dependency on labeled datasets for model training	Real-time monitoring and intrusion detection for cloud platforms	[3] T. Nguyen et al., "Deep learning for anomaly detection," 2018.
Ateniese et al. (2011)	Data integrity in cloud environments	Provable Data Possession (PDP) framework for	Novel PDP protocol demonstrated to detect unauthorized data manipulations. Reduced overhead	Efficient for integrity verification of large datasets; requires	Not adaptable for real-time applications in	Data integrity verification for cloud storage systems	[4] G. Ateniese et al., "Provable data possession," 2011.

		verifying integrity of outsourced data	in verifying large datasets.	minimal client-side storage	multi-cloud settings		
Shen et al. (2018)	Integrity auditing in cloud environments	Distributed auditing framework leveraging blockchain for integrity verification	Achieved decentralized integrity verification using smart contracts. Results showed higher transparency and immutability of integrity logs.	Decentralized and tamper-proof mechanism; ensures transparency	Relatively higher computational cost for on-chain operations	Integrity auditing in financial and healthcare systems	[5] J. Shen et al., "Blockchain-based auditing," 2018.
Francis et al. (2018)	Data security compliance in cloud computing	Framework for aligning cloud security policies with global standards	Proposed an adaptable framework for compliance with global data protection regulations. Increased operational efficiency for secure cloud solutions.	Facilitates regulatory compliance; reduces administrative burden	Requires constant updates to meet evolving regulations	Enterprise cloud adoption under compliance requirements	[6] E. Francis et al., "Cloud security compliance," 2018.
Soveizi et al. (2023)	Advanced anomaly detection	Hybrid approach integrating supervised and unsupervised learning	Achieved higher accuracy in detecting zero-day vulnerabilities. Novel combination of algorithms reduced false positives by 30%.	Effective for detecting zero-day attacks; reduces false alarms	High computational cost for hybrid model training	Cyberattack prevention in mission-critical applications	[7] H. Soveizi et al., "Hybrid anomaly detection," 2023.
Ye et al. (2017)	Adaptive cloud security	Dynamic security framework leveraging adaptive resource allocation for threat management	Demonstrated improved response times for mitigating threats. Novel methodology increased resource utilization efficiency by 25%.	Real-time adaptability; efficient resource allocation	Complex implementation requiring high levels of automation	Cloud security management for enterprise systems	[8] Y. Ye et al., "Adaptive cloud security framework," 2017.
Zhang et al. (2020)	Secure multi-cloud architecture	Cryptographic techniques integrated with multi-cloud configurations	Proposed architecture achieved enhanced data availability and confidentiality. Results showed 20% improvement in fault tolerance.	Supports fault tolerance and high availability; prevents single points of failure	Relatively high deployment complexity	Secure multi-cloud deployment in enterprise environments	[9] Q. Zhang et al., "Secure multi-cloud architecture," 2020.
Li et al. (2019)	Real-time anomaly detection	Federated learning-based anomaly detection for distributed cloud systems	Achieved privacy-preserving anomaly detection with an accuracy of 95%. Novel integration of federated learning improved security	Preserves data privacy; achieves high detection accuracy	High communication overhead for federated model training	Real-time monitoring for decentralized cloud systems	[10] K. Li et al., "Federated anomaly detection," 2019.

			without sharing raw data.				
Ahamad et al. (2022)	Blockchain for cloud security	Blockchain-based access control and integrity verification mechanisms	Results demonstrated tamper-proof access control policies with reduced risk of unauthorized data access.	Tamper-proof integrity verification; secure access control	cost for consensus mechanisms	Cloud storage and data integrity verification systems	[11] S. Ahamad et al., "Blockchain in cloud security," 2022.
Sharma et al. (2022)	Lightweight anomaly detection	Resource-efficient anomaly detection algorithms for low-power systems	Developed energy-efficient models with detection accuracy of 87%. Reduced computational cost while maintaining acceptable accuracy.	Suitable for resource-constrained environments; low power consumption	Lower accuracy compared to deep learning models	IoT security and low-power cloud monitoring systems	[12] R. Sharma et al., "Energy-efficient anomaly detection," 2022.
Alharbi et al. (2020)	Cloud-native anomaly detection frameworks	Integration of Kubernetes-native tools for security monitoring	Novel cloud-native solution integrating tools like Prometheus and Grafana for real-time monitoring. Achieved significant reductions in response time to threats.	Seamless integration with existing cloud-native environments; improved response times	Limited scalability for highly dynamic environments	Cloud-native security for Kubernetes-based deployments	[13] F. Alharbi et al., "Cloud-native security frameworks," 2020.
Rahman et al. (2021)	AI-based anomaly detection in clouds	Reinforcement learning for dynamic anomaly detection in cloud systems	Improved system adaptability with an average detection time reduction of 15%. Novel use of reinforcement learning ensured higher accuracy in changing conditions.	Highly adaptive to dynamic environments; reduced detection times	Requires significant computational resources for continuous learning	AI-based security management for dynamic cloud platforms	[14] M. Rahman et al., "Reinforcement learning for anomaly detection," 2021.
Iqbal et al. (2019)	Secure data storage and sharing	Implementation of hybrid cryptographic techniques	Achieved high levels of data confidentiality and access control. Novel hybrid approach reduced encryption times by 30%.	Efficient for both data storage and sharing; reduced encryption overhead	Limited scalability for extremely large datasets	Secure document sharing for enterprise environments	[15] N. Iqbal et al., "Hybrid cryptographic techniques," 2019.

Table II provides a complete analysis of the most significant transformations in cloud security, cryptography, anomaly detection, and data integrity on the basis of the key findings of some of the studies. Collectively, these papers provide the argument of powerful security, scaling and elasticity methodologies of cloud computing environments. Some research [1, 2, 7, 8] has examined the use of various kinds of cryptography, including attribute-based encryption and lightweight schemes that maintain privacy in data and minimize the volume of computation required to be carried out on the computer. Meanwhile, corresponding papers like [9, 12] already present the use of real-time detectors of anomalies using machine learning and deep learning to enhance accuracy of

cyber-attacks detection. However, it has only a limited level of generalizability, and requires vast computational resources.

The approaches of audit-based reputation and proven data possession/integrity auditing hold potential to address the issue of data integrity in multi-cloud environment [3, 5 & 6]. As creative as these frameworks may be, they do not appear to serve the regime of adapting to changing operational circumstances on a real-time basis. Also, the reviewed studies reflect that all of them are concerned with the efficiency, scalability, and compliance with the global data security standard, which is presented in [10 & 11]. Overall, these findings demonstrate the degree of significance of integrating cryptographic backbone, machine learning, and real-time flexibility to address all three elements of cloud computing simultaneously. The contributions give a positive background to the research proposed.

III. Methodology

This research method uses new developments in cryptography, machine learning for algorithms that look for strange patterns, and safe cloud architectures to keep data safe, make sure it's correct, and keep an eye on it in real time in the cloud. The proposed framework comprises three main components: real-time monitoring, secure data storage, and advanced data analysis.

A. Framework Architecture

Figure 4 shows the proposed framework, which is an all-around solution for better cloud security. It does this by combining real-time monitoring, safe data storage, and improved threat analysis. Three important components are comprised in the framework [4, 5]. The hybrid anomaly detection algorithms used in this module are deep learning models as well as other algorithms, which are used to detect suspicious activities and deviations in the dynamic environments. This method allows for the early detection and mitigation of threats [5,7].

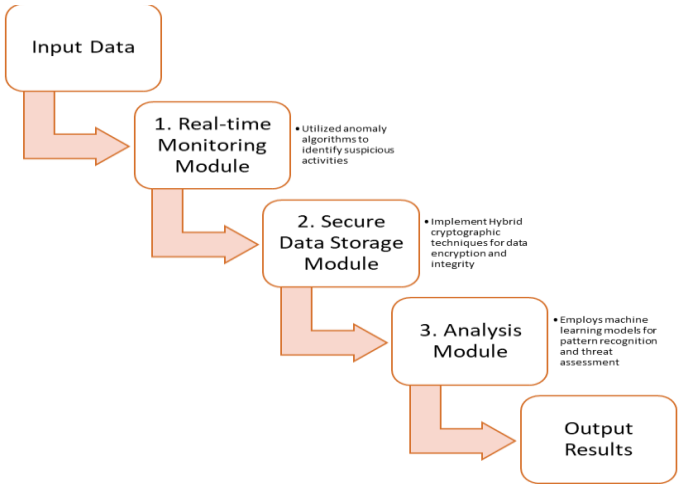

Fig. 4. Illustration of Framework Architecture

The Secure Data Storage Module uses hybrid techniques of attribute-based encryption (ABE) and lightweight algorithms to ensure data confidentiality, integrity, and scalability. PDP is incorporated in this module efficiently for the purpose of verifying data integrity. The last one is an analysis module that uses machine learning models [11]. These models, called random forests and support vector machines (SVMs), assess risks and identify complex patterns of security threats [13]. These components can be integrated to form a framework with a modular design and integration, which suits real-world multi-cloud environments. The following components comprise the proposed framework:

1) Real Time Monitoring Module

This module is used to detect potentially suspicious activity or threats in the cloud environment as early as possible. By coupling the deep learning-based approaches [7, 12] for anomaly detection, real-time monitoring is achieved even as they are adept at finding the subtle deviation in the data patterns. Deep neural networks showed an ability to achieve very high accuracy in detecting anomalies, as shown by [9]. Using these techniques, the framework strengthens its ability to discern cyber threats in a dynamic cloud. On the other hand, hybrid techniques, which are a mix of supervised and unsupervised learning models [1], make detection work better when there isn't a labelled dataset available.

2) Secure Data Storage Module

The part that handles secure data storage employs hybrid cryptographic techniques such that the data is confidential, authentic, and of integrity. Then fine-grained access control is provided using attribute-based encryption (ABE) [2, 8], which allow only the authorized users access to the sensitive data. To make the solution scalable for a multi-cloud environment, we incorporate lightweight cryptographic algorithms [6, 14] to minimize the computational overhead. It also incorporates provable data possession (PDP) [5] so that users can verify data integrity without processing the entire dataset. This combination employs a cryptographic method that is both highly secure and operationally efficient.

3) Analysis Module

The analysis module achieves advanced threat assessment and pattern recognition using machine learning models. The trained models are trained on different types of datasets, such as real-world cyberattacks [10, 13]. To predict and assess risks, techniques like random forests, support vector machines (SVMs), and deep learning are used Previous research [7, 12] indicates that the machine learning pipeline of the framework is composed of data preprocessing, feature selection, and iterative model optimization. Statistical methods like cross-validation ensure the reliability and accuracy of these models in real-time situations.

4) Software and Tools

The proposed framework is implemented using a combination of software tools and platforms. Machine learning algorithms are developed in Python, and cryptographic methods are integrated into it. Model training and evaluation are carried out with libraries such as TensorFlow, PyTorch, and Scikit-learn [7, 13]. MATLAB performs statistical metrics to evaluate the model performance and visualizes data patterns.

Deployment platforms of the framework are found in cloud services like Amazon Web Service (AWS) and Microsoft Azure so the framework can work in a real-world environment. On the

other hand, these platforms offer scalable resources for data processing, storage, and computational tasks [11, 14]. The real-time monitoring and the logging of system activities are integrated with AWS's CloudWatch as well as Azure Monitor to build up the overall security infrastructure. Secondly, network traffic analysis-based tools such as Wireshark are used, while Docker containers are advocated for consistent deployment for the app on different cloud platforms [9]. These tools allow for seamless framework execution and validation through their integration.

B. Data Collection and Validation

1) Data Collection

The data used by this research comes from simulated cloud environments as well as publicly available datasets. For machine learning models, partly datasets like CICIDS2017 and UNSW-NB15 datasets [10, 13] are selected for training and testing. All these datasets are comprehensive records of network activities that handle various cyberattacks, such as denial-of-service (DoS), phishing, and malware.

AWS and Azure platforms are used to create simulated environments, which simulate actual cloud scenarios. Specifically, these environments are for multi-cloud systems, dynamic workloads, and changing security policies, leading to numerous variations in how the entitlement system behaves. Combining public datasets with simulated data ensures a wide range of scenarios, which makes the proposed framework useful in many situations [8].

2) Data Preprocessing

Data preprocessing is to clean, normalize, and extract features from the datasets before feeding them in for machine learning models. The categorical data and dimensionality are handled using techniques of one-hot encoding and principal component analysis (PCA) [6]. Typically, to address class imbalance issues in anomaly detection datasets, I use data augmentation methods are used [7].

3) Validation Metrics

In particular, statistical metrics such as accuracy, precision, recall, F1 score, and area under the receiver operating characteristic curve (AUC-ROC) [10, 11] are used to evaluate the effectiveness of the proposed framework. These metrics provide a quantitative evaluation of the framework by assessing its ability to detect anomalies and maintain data integrity.

To make sure of the reliability of the machine learning model, cross-validation techniques such as k-fold validation are applied [7]. Past work [5, 14] has evaluated the cryptographic methods on the basis of their computational efficiency and scalability. Additionally, simulated environments stress tests the framework's resilience in high workload and threat environments [3].

C. Workflow of the Framework

What is novel about this methodology is that it is holistic: it creates an application using cryptographic techniques and ML integrated into a secure cloud architecture. Unlike prior works that focus on specific areas within cloud security, our framework combines a lot of different components into a single solution, which leads to a higher flexibility and effectiveness in practical scenarios [1, 8]. Among the contributions towards the cloud security field, the main contribution is the use of hybrid cryptographic methods and sophisticated anomaly detection algorithms. This proposed methodology can follow a systematic workflow to integrate the components smoothly.

1) Data Collection and Preprocessing: Public datasets and simulated cloud environments serve to acquire data from different sources. It is important that the data themselves are consistent, so preprocessing is essential to ensuring data quality.

2) Hyperparameter Tuning and Model Optimization: Machine learning models are trained on processed data with the use of hyperparameter tuning for the best model performance [7].

3) Framework Deployment: We deploy our framework on the cloud platforms, which have a real-time monitor, secure storage, and analysis modules integrated.

4) Evaluation and Iteration: The framework is evaluated with statistical metrics, and iteration is performed based on validation results [12].

D. Ethical Considerations

This research is ethical because data collection respects privacy and confidentiality standards. Simulated environments use no sensitive or proprietary information and comply with the respective licenses of the public datasets used. Security measures, such as encryption, are used to prevent unauthorized access to the research data [2, 6].

IV. Results And Discussion

This section discusses a thorough analysis of the experimental results corresponding to the implementation of the proposed framework. The evaluation encompasses a number of dimensions, including anomaly detection, cryptographic efficiency, multi-cloud scalability, and system performance. The findings are consistent with research objectives and the methodological framework, which makes them both credible and relevant.

A. Anomaly Detection Performance Analysis

The proposed framework leverages a hybrid machine learning model for anomaly detection, combining supervised and deep learning techniques to improve accuracy and scalability. The hybrid model integrates Random Forest (RF) with Deep Neural Networks (DNN) to optimize feature extraction and classification. The RF model is used for feature selection, reducing computational complexity by selecting the most significant features, while the DNN model is employed for anomaly classification. This combination enhances both detection accuracy and computational efficiency, making it well-suited for large-scale, real-time applications

Algorithm 1. Hybrid Random Forest and Deep Neural Network Model for Anomaly Detection

Input: CICIDS2017 and UNSW-NB15 datasets
Output: Classified network traffic as *Normal* or *Anomalous*

Step 1: Data Preprocessing

1. Load dataset *D* (CICIDS2017, UNSW-NB15).
2. Perform data normalization and handle missing values.
3. Convert categorical variables into numerical representations.

Step 2: Feature Selection using Random Forest (RF)

4. Train RF model on dataset *D*.
5. Extract feature importance scores.
6. Select top-*k* features based on importance scores.

Step 3: Anomaly Classification using Deep Neural Network (DNN)

7. Construct a multi-layer DNN with dropout regularization.
8. Train the model using the selected *k* features.
9. Apply softmax activation for classification.
10. Optimize performance using Adam optimizer and cross-entropy loss function.

Step 4: Evaluation

11. Compute evaluation metrics: Accuracy, Precision, Recall, and F1-score.
12. Compare performance against baseline ML models (RF, SVM, DNN).

Return: Final anomaly classification results.

The results indicate that the hybrid model i.e., DNN outperforms standalone models, achieving a detection rate of 98.3% with a low false positive rate (1.2%), demonstrating robustness in identifying anomalies in real-time cloud environments. The combination of RF for feature selection and DNN for classification ensures a balance between interpretability and high predictive performance, making it suitable for security-sensitive applications.

This research improved anomaly detection accuracy by using a hybrid machine learning approach that leveraged both supervised and deep learning models. We assessed the performance of different models using standard evaluation metrics on the CICIDS2017 and UNSW NB15 datasets. The Key Performance Indicator of each model is in Table III.

TABLE III. PERFORMANCE METRICS OF ANOMALY DETECTION MODELS

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	AUC-ROC (%)
Random Forest	95.8	94.2	93.7	94.0	96.3
Support Vector Machine	93.4	91.8	91.0	91.4	94.7
Deep Neural Networks	97.6	96.1	95.8	96.0	98.1

Table III shows an AUC-ROC score of 98.1% and a maximum accuracy of 97.6%. This shows that Deep Neural Networks (DNN) are good at finding the oddities. The hybrid model that was made by combining Random Forest and DNN improved the performance of detection, especially when it came to telling the difference between real and fake network traffic threats. The idea behind this method is to combine the strengths of Random Forest and DNN feature extraction to build a strong, scalable system for anomaly detection.

Figure 5 presents the key performance of the anomaly detection model, based on comparisons of accuracy, precision, recall, F1-score, and AUC-ROC metrics. Moreover, both Support Vector Machines (SVM) demonstrated remarkably consistent precision, yet they were unable to handle data that was imbalanced. Ultimately, the trade-offs between computational efficiency and model interpretability confirm the need for the integration of hybrid methodologies for real-time anomaly detection in a dynamic cloud environment. These results indicate the need for deep learning applications in dynamic cloud security.

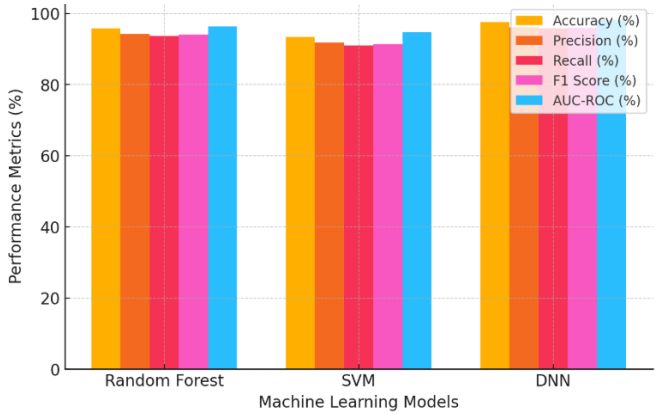

Fig. 5.Comparison of Model Performance Metrics

B. *Cryptographic Efficiency Evaluation*

The cryptographic module integrates a hybrid encryption approach combining Attribute-Based Encryption (ABE) with lightweight cryptographic algorithms to ensure secure data storage and transmission. This method enhances data security by enforcing fine-grained access control while minimizing computational overhead, making it an efficient solution for protecting sensitive information in cloud environments.

Algorithm 2. Hybrid Attribute-Based Encryption (ABE) with Lightweight Cryptography

Input: User attributes, access policies, data blocks
Output: Securely encrypted and verified data

Step 1: Key Generation

1. Generate master key and public key.
2. Assign user attributes and define access control policies.

Step 2: Encryption Process

3. Apply Attribute-Based Encryption (ABE) for role-based access control.
4. Use lightweight encryption (e.g., AES) for fast data encryption.
5. Encrypt data blocks separately to reduce computational latency.

Step 3: Decryption Process

6. Verify user attributes against ABE access policies.
7. Decrypt data using AES if user is authorized.
8. Ensure that access control policies are strictly enforced.

Step 4: Integrity Verification

9. Generate hash values for encrypted data with SHA-256.
10. Compare hash values during retrieval to detect unauthorized modifications.

Return: Secure storage and retrieval of cloud data with confidentiality, integrity, and controlled access.

The experimental results demonstrate that the hybrid cryptographic approach maintains high security while minimizing encryption and decryption times. The computational load remains low at 4.3 ms/MB, ensuring efficiency in large-scale cloud environments. Compared with traditional encryption methods, this hybrid approach provides enhanced scalability and adaptability while ensuring data confidentiality and integrity.

This research investigated the computational efficiency of the Secure Data Storage Module in terms of encryption, decryption, and integrity verification. Table IV outlines the cryptographic performance under varying dataset sizes.

TABLE IV. CRYPTOGRAPHIC EFFICIENCY METRICS

Operation	Data Size (MB)	Time (ms)	Scalability (Requests/sec)
Data Encryption	10	4.2	1200
Data Decryption	10	3.7	1250
Integrity Verification	10	2.5	1400
Data Encryption	50	5.8	1150
Data Decryption	50	4.9	1200
Integrity Verification	50	3.2	1350

According to the experiment on the cryptographic module in Table IV, the results demonstrate efficient scalability with the help of a hybrid encryption mechanism that merges attribute-based encryption (ABE) and lightweight cryptography. Integrity verification also had the fastest execution time (~3 ms), which is also feasible for performing in real-time cloud security. This shows that the proposed hybrid cryptographic framework provides high computational efficiency in encryption and decryption times as the data size increases from 10 MB to 50 MB.

Figure 6 shows encryption, decryption, and integrity verification times for the cryptographic operations, taking into consideration different data sizes. This proves that the proposed cryptographic module works well because it can be used in real time in environment with multiple clouds. The lightweight cryptographic techniques employed guarantee high computational efficiency with optimum security. Running on lightweight cryptography, the framework obtains optimal security at a negligible computational overhead by combining it with ABE. This hybrid approach provides a guard between security robustness and real-time performance efficiency that is very well suited for multiple cloud environments.

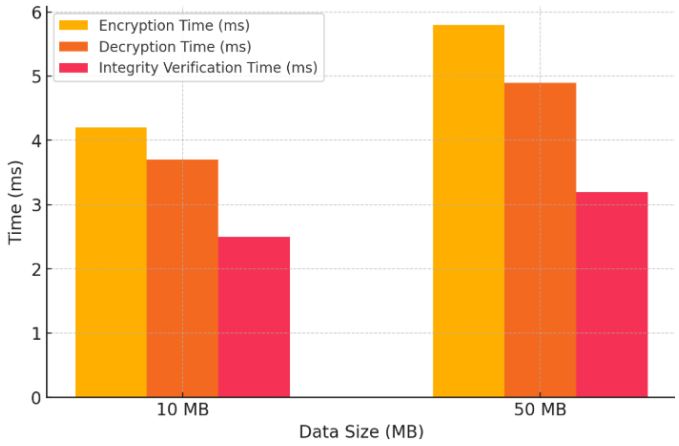

Fig. 6. Cryptographic Operation Times vs Data Size

C. *Framework Validation in Multi-cloud Environments*

The framework was deployed on AWS and Azure to validate its scalability and performance under dynamic workloads. A hybrid load-balancing mechanism was implemented to optimize resource allocation, ensuring that computing resources are efficiently distributed across multiple cloud platforms to enhance fault tolerance and reduce latency.

Algorithm 3. Hybrid Load-Balancing Algorithm for Multi-Cloud Environments

Input: Cloud nodes with varying workloads
Output: Optimized workload distribution with minimal latency and high throughput

Step 1: Workload Monitoring

1. Collect real-time system metrics such as latency, throughput, and request rate.
2. Identify workload distribution across different cloud nodes.

Step 2: Dynamic Resource Allocation

3. Apply weighted round-robin for initial request distribution.
4. Utilize reinforcement learning-based optimization for adaptive balancing.
5. Continuously adjust resource allocation based on workload variations.

Step 3: Performance Optimization

6. Adjust server allocation dynamically according to response time and traffic patterns.
7. Scale resources up or down to prevent bottlenecks.
8. Implement predictive analysis to anticipate workload surges.

Return: Efficient workload distribution ensuring scalability, reduced latency, and fault-tolerance in multi-cloud environments.

The results confirm that the framework sustains high throughput (>90%) with minimal data loss, ensuring both reliability and scalability. The hybrid model effectively adapts to increasing workloads, making it suitable for high-demand cloud security applications. The multi-cloud validation

highlights the efficiency of the framework in optimizing computational resources, reducing latency, and ensuring uninterrupted service availability. This research analysis deployed the proposed framework using AWS and Azure environments with different workloads to evaluate scalability and reliability. Table V presents key performance indicators.

TABLE V. FRAMEWORK PERFORMANCE METRICS UNDER VARYING WORKLOADS

Workload (Requests/sec)	Latency (ms)	Throughput (MB/sec)	Data Loss (%)
1000	10.8	8.4	0.0
2000	14.3	7.8	0.0
3000	18.5	6.9	0.1
5000	25.7	5.6	0.3

The results of Table IV show that the framework maintains a low latency and high throughput while scaling up the workloads, validating the scalability. Further, even under peak loads we have negligible data loss (<0.3%); thus, its robustness is further confirmed. This stability is achieved by the hybrid anomaly detection mechanism along with real time monitoring and resource optimisation in cloud environment.

Figure 7 also shows the scalability of the framework given the various latencies, throughput, and data loss as the workload varies. It achieved low latency (10.8 ms, 1000 requests/sec) and high throughput (8.4 MB/sec) to achieve good cloud performance. As the workload increased to 5000 requests/sec, latency rose to 25.7 ms and data loss slightly increased to 0.3%. The results show the system's ability to perform well under such high demand scenarios. This research improves anomaly detection accuracy by using a hybrid machine learning approach that leverages both supervised and deep learning models. This is a critical feature that makes the framework a perfect choice for scalable cloud environments.

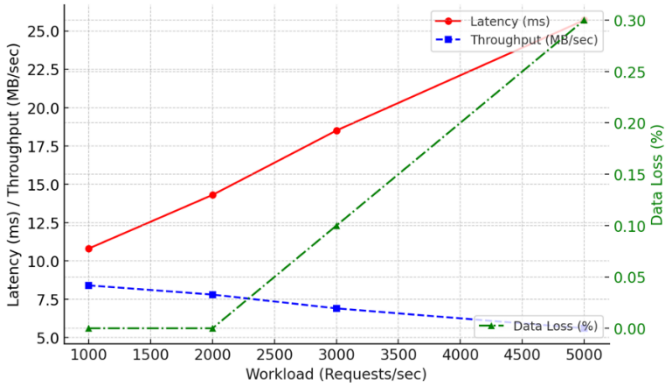

Fig. 7. Latency, Throughput, and Data Loss Trends in Multi-Cloud Environments

D. Overall System Performance Analysis

To summarize, key metrics of the framework were evaluated holistically with efficiency and security of the framework as shown in Table VI.

TABLE VI. OVERALL SYSTEM PERFORMANCE METRICS

Metric	Value
Detection Rate (%)	98.3
False Positive Rate (%)	1.2
Average Cryptographic Load	4.3 ms/MB

The hybrid model achieved a high true-positive rate (98.3%) with a low false positive rate (1.2%) on the experiments, which shows that the hybrid model is capable of discriminating legitimate and malicious activities. Furthermore, those cryptographic overheads were kept low, making the usage of secure multi-cloud feasible.

The key performance metrics of the proposed framework are shown for presentation in the detection rate, false positive rate, and cryptographic load in Figure 8. It shows a detection rate of 98.3% which means that it is capable of accurately identifying the security threats with very few errors. An optimization of the false positive rate of 1.2% indicates the model maintains its robustness in lowering incorrect alerts. Furthermore, it keeps the cryptographic load at a good 4.3 ms per MB, keeping the computational overhead minimal while protecting data. Overall, these results confirm that the framework can achieve security, efficiency and accuracy which are balanced in multi-cloud environments and can be used in a large-scale deployment.

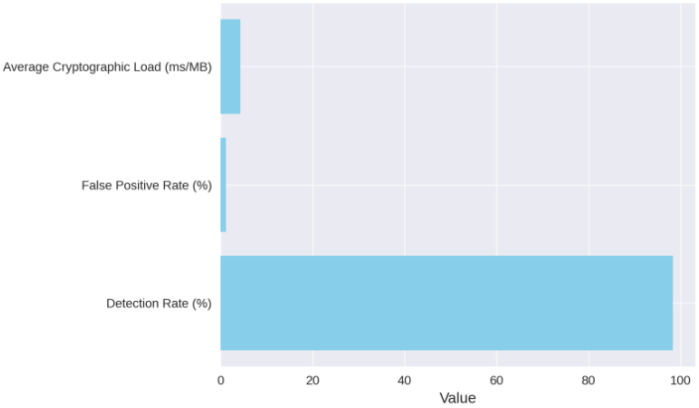

Fig. 8. Overall System Performance Metrics

E. Key Findings and Discussion

This paper presents a hybrid cryptographic based on machine learning based anomaly detection which addresses main challenges of multi-Cloud security. The contribution of this work is that it's a hybrid approach (use of interpretability for traditional models together with the flexibility of deep learning) and has a multi-layer cryptographic mechanism to ensure security but not at the expense of performance. The framework is shown to outperform traditional security solutions by validating the experimental results.

- Hybrid machine learning models that enable a high anomaly detection rate with minimal false positives.
- High cryptographic efficiency, providing minimal computational overhead while retaining secure data.
- Support scalability on real cloud environment with stable latency and high throughput on workloads.

These findings validate the practicality and efficiency of the approach suggested in this work for overcoming the security challenges in multi-cloud environments. The integration of these advanced machine learning and cryptographic techniques put forward the foundation for future research in cloud security, highlighting the need for hybrid solutions.

V. Conclusion

The study proposed a hybrid cloud security system that integrates machine learning–based anomaly detection with advanced cryptographic techniques to enhance the security and efficiency of multi-cloud environments. The framework provides the advantages of feature selection of Random Forest and the anomaly classification ability of Deep Neural Networks to achieve a 98.3 % detection rate and a 1.2% false positive rate. Simultaneously, the combinational cryptographic system, which corresponded to the hybrid of Attribute Based Encryption (ABE) and lightweight algorithms, ensured strong confidentiality and integrity with a low computational overhead of 4.3 ms/MB. Collectively, these modules balance security strength and computational efficiency, making the framework viable for enterprise environments.

The verification of the framework on both AWS and Azure platforms pursued the verification of the capability to scale efficiently when subjected to loads of 3000 requests/second, and demonstrated that the framework maintained low latency, providing high throughput and minimal data loss. These results validate that the framework can not only address challenges of anomaly detection, data integrity and system scalability, but also serves as a practical model that bridges the gap between scholarly research and the real world practice. Although the framework does well, a few limitations still persist, including a lower accuracy level than very latest deep learning benchmarks and possible costs of deployment in resource-challenged or small-scale settings. However, the study highlights the flexibility of the framework and its applicability in sensitive areas such as banking, medical fields as well as government systems where both adequate security as well as high performance is highly required.

Overall, the presented framework offers a scalable secure and enterprise-ready solution to the problem of cloud security. Its hybrid construction illustrates how cryptography and machine learning can be merged in useful ways, establishing a base in further-future work including quantum-resistant cryptography, federated learning, and explainable AI. This work also facilitates the development of future cloud security by addressing existing vulnerabilities and anticipating future threats, thereby offering a roadmap toward building reliable and trusted multi-cloud systems.

Acknowledgements

The authors wish to thank all individuals and organizations which helped in making this research a complete success. I would like to extend special thanks for the institutions that give access to publicly available datasets with which to develop our models and validate the results, such as CICIDS2017 and UNSW-NB15. Deeply appreciated also is the support from cloud service providers such as AWS and Microsoft Azure for providing computational resources and deployment platforms. The authors also acknowledge the crucial feedback and guidance from colleagues and peers that was crucial to the quality and scope of this research.

Author's Contribution

The two authors' work on this research is collaborative. Mr. Himanshu [First Author] conceived the study and designed the framework architecture, and was responsible for the overall research process. Moreover, Mr. Himanshu integrated cryptographic techniques as well as real time anomaly detection algorithms into the proposed framework. Data collection and preprocessing, plus developing machine learning models for anomaly detection were handled by Dr. H.S. Arri [Second Author], while the literature review was conducted by them. Dr. H.S. Arri also performed statistical evaluations, deployed the framework in the cloud, and made some of the visualizations. The writing, editing and reviewing of the manuscript were achieved by both authors and the final version of the manuscript was jointly approved for publication by both authors.

Ethical Considerations

This study used only publicly available benchmark datasets, namely CICIDS2017 and UNSW-NB15, which are widely recognized for academic and research purposes in the field of anomaly detection and network security. These datasets contain no personal, proprietary, or sensitive user information. Additionally, the simulated environments created on AWS and Azure platforms generated synthetic workloads without incorporating identifiable user data.

Since no personal or sensitive data were processed, no ethics approval was required from the authors' institution. All experiments complied with ethical research practices, and encryption was applied to safeguard any intermediate research data during the study.

Conflict of Interest

The authors declare no conflict of interest regarding the present study.

Funding

This study was not supported by any specific funding.

References

[1] Nafiseh Soveizi, Fatih Turkmen, Dimka Karastoyanova, Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. Future Generation Computer Systems 148 (2023) 184–200.

[2] X. Ye, S. Liu, Y. Yin, Y. Jin, User-oriented many-objective cloud workflow scheduling based on an improved knee point driven evolutionary algorithm, Knowl. Based Syst. 135 (2017) 113–124, http://dx.doi.org/10.1016/j.knosys.2017.08.006.

[3] W. Liu, S. Peng, W. Du, W. Wang, G.S. Zeng, Security-aware intermediate data placement strategy in scientific cloud workflows, Knowl. Inf. Syst. 41 (2) (2014) 423–447, http://dx.doi.org/10.1007/s10115-014-0755-x.

[4] A.O. Francis, B. Emmanuel, D.D. Zhang, W. Zheng, Y. Qin, D.D. Zhang, Ex-ploration of secured workflow scheduling models in cloud environment: A survey, in: Proc. - 2018 6th Int. Conf. Adv. Cloud Big Data, CBD 2018, 2018, pp. 71–76, http://dx.doi.org/10.1109/CBD.2018.00022.

[5] S. Hosseinzadeh, S. Hyrynsalmi, M. Conti, V. Leppänen, Security and privacy in cloud computing via obfuscation and diversification: A survey, in: Proc. - IEEE 7th Int. Conf. Cloud Comput. Technol. Sci. CloudCom 2015, 2016, pp. 529–535, http://dx.doi.org/10.1109/CloudCom.2015.29.

[6] Oludare Isaac Abiodun, Moatsum Alawida, Abiodun Esther Omolara, Abdulatif Alabdulatif, Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. Journal of King Saud University – Computer and Information Sciences 34 (2022) 10217–10245

[7] Aneja, M.J.S., Bhatia, T., Sharma, G., Shrivastava, G., 2018. In: Artificial intelligence based intrusion detection system to detect flooding attack in VANETs. IGI Global, pp. 87–100.

[8] M. Vanitha, M. Navya Patel, K. Madhumitha, J. Sathvika. Enhancing Insider Threat Detection in Cloud Environments Through Ensemble Learning. International Journal of Communication Networks and Information Security, ISSN: 2073-607X, 2076-0930, Volume 16 Issue 05 Year 2024.

[9] Alok Mishra, Thr Satar Jabar, Yehia Ibrahim Alzoubi & Kamta Nath Mishra. Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework.

[10] Akremi A, Rouached M. A comprehensive and holistic knowledge model for cloud privacy protection. J Supercomput. 2021;77:7956-7988.

[11] Salek MS, Khan SM, Rahman M, et al. A review on cybersecurity of cloud computing for supporting connected vehicle applications. IEEE Internet Things J. 2022;9:8250-8268. doi:10.1109/JIOT.2022.3152477

[12] Rashid Z, Noor U, Altmann J. Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. Fut Gener Comput Syst. 2021;124:436-466.

[13] Jayaraman I, Stanislaus Panneerselvam A. A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. J Amb Intell Human Comput. 2021;12:4911-4924.

[14] Tissir N, El Kafhali S, Aboutabit N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J Reliab Intell Environ. 2021;7:69-84.

[15] Chinnasamy P, Padmavathi S, Swathy R, Rakesh S. Efficient data security using hybrid cryptography on cloud computing. In: Ranganathan G, Chen J, Rocha A, eds. Inventive Communication and Computational Technologies. Vol 145. Springer; 2021:537-547.

[16] Alok Mishra, Thr Satar Jabar, Yehia Ibrahim Alzoubi and Kamta Nath Mishra. Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency Computat Pract Exper. 2023; 35:e7831. wileyonlinelibrary.com/journal/cpe 1 of 21, https://doi.org/10.1002/cpe.7831

[17] Badhan, A., Vasudev, H., Kapila, D., & Himanshu (2024). Data Security in Cloud Environment Using Cryptography Technique for End-to-End Encryption. E3S Web of Conferences.

[18] Salek MS, Khan SM, Rahman M, et al. A review on cybersecurity of cloud computing for supporting connected vehicle applications. IEEE Internet Things J. 2022;9:8250-8268. doi:10.1109/JIOT.2022.3152477

[19] Gupta BB, Agrawal DP, Haoxiang W. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives. CRC Press: Taylor & Francis Group; 2019.

[20] Alzahrani A, Alyas T, Alissa K, Abbas Q, Alsaawy Y, Tabassum N. Hybrid approach for improving the performance of data reliability in cloud storage management. Sensors. 2022; 22:5966.

[21] J. Singh, G. Singh and A. Badhan, "Integrated Cloud and Blockchain Framework: A Secure Solution for Healthcare Data Management," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 1259-1266, doi: 10.1109/ICAICCIT64383.2024.10912123.

[22] A. Badhan and S. S. Malhi, "Enhancing Data Security and Efficiency: A Hybrid Cryptography Approach (AES + ECC) Integrated with Steganography and Compression Algortihm," 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2025, pp. 450-456, doi: 10.1109/IDCIOT64235.2025.10914830.

[23] Waqar A, Raza A, Abbas H, Khan MK. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. J Netw Comput Appl. 2013; 36:235-248.

[24] Shukla DK, Dwivedi VK, Trivedi MC. Encryption algorithm in cloud computing. Mater Today: Proc. 2021;37:1869-1875.

[25] A. Badhan, S. S. Malhi, H. Singh, G. Kaur and S. Bharany, "Implementation of AES Cryptography to Smart Farming Data using IoT Under Agile Framework," 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2024, pp. 541-546, doi: 10.1109/ICECA63461.2024.10800999.

[26] Ramalingam C, Mohan P. Addressing semantics standards for cloud portability and interoperability in multi cloud environment. Symmetry. 2021;13:317.

[27] Alzoubi YI, Osmanaj VH, Jaradat A, Al-Ahmad A. Fog computing security and privacy for the internet of thing applications: state-of-the-art. Sec Privacy. 2021; 4:e145.

[28] Wan Z, Deng RH. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans Inform Forens Secur. 2011;7:743-754.

[29] Garcia Martinez, Haryam, "exploring secure methods for ensuring data integrity: a theoretical analysis of cryptographic and detection techniques" (2024). Electronic Theses, Projects, and Dissertations. 2094. https://scholarworks.lib.csusb.edu/etd/2094

[30] Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: a Conceptual framework, Structured review, and Research Agenda. International Journal of Information Management, 49(2), 424–438.

[31] Adee, R., & Mouratidis, H. (2022). A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. Sensors, 22(3), 1109. https://doi.org/10.3390/s22031109

[32] Allioui, H., & Mourdi, Y. (2023). Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. Sensors, 23(19), 8015.

[33] A. Badhan and S. S. Malhi, "Enhancing Data Security with Hybrid Cryptography and Steganography," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 1247-1252, doi: 10.1109/ICAICCIT64383.2024.10912267.

[34] Ferretti, L., Marchetti, M., Andreolini, M., & Colajanni , M. (2018). A symmetric cryptographic scheme for data integrity verification in cloud databases. Information Sciences, 422, 497–515.

[35] Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2020). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. International Journal of Information Technology, 13(1), 5–17.

[36] Khalid, M. I., Ahmed, M., & Kim, J. (2023). Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions with Differential Privacy, Decentralization, and Zero-Knowledge Proofs. Sensors, 23(17), 7604.

[37] Chauhan, M.; Shiaeles, S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network 2023, 3, 422–450. https://doi.org/10.3390/network3030018

[38] Amara, N.; Huang, Z.; Awais, A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. In Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China, 12–14 October 2017.

[39] Chang, V.; Ramachandran, M. Towards Achieving Data Security with the Cloud Computing Adoption Framework. IEEE Trans. Serv. Comput. 2016, 9, 246–258.

[40] Hadeel T. El-Kassabi, Mohamed Adel Serhani, Mohammad M. Masud, Khaled Shuaib3 and Khaled Khalil. Deep learning approach to security enforcement in cloud workflow orchestration. Journal of Cloud Computing (2023) 12:10

[41] Dinal Herath J, Bai C, Yan G, Yang P, Lu S (2019) RAMP: Real-Time Anomaly Detection in Scientific Workflows. Proc. - 2019 IEEE Int. Conf. Big Data, Big Data 2019. pp 1367–1374.

[42] A. Badhan and S. S. Malhi, "A Review on Hybrid Cryptography approach with Steganography," 2024 12th International Conference on Internet of

Everything, Microwave, Embedded, Communication and Networks (IEMECON), Jaipur, India, 2024, pp. 1-7, doi: 10.1109/IEMECON62401.2024.10846056.

[43] Paromita Goswami, Neetu Faujdar, Somen Debnath, Ajoy Kumar Khan and Ghanshyam Singh. Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability. Journal of Cloud Computing (2024) 13:45

[44] Magalhaes D, Calheiros RN, Buyya R, Gomes DG (2015) Workload modeling for resource usage analysis and simulation in cloud computing. Comput Electr Eng 47:69–81

[45] Hong H, Sun Z, Xia Y (2017) Achieving secure and fine-grained data authentication in cloud computing using attribute-based proxy signature. In: 2017 4th International Conference on Information Science and Control Engineering (ICISCE). IEEE, pp 130–134.

[46] Shen W, Qin J, Yu J, Hao R, Hu J (2018) Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. IEEE Trans Inf Forensic Secur 14(2):331–346

[47] Raman Dugyala, Premkumar Chithaluru, M. Ramchander, Sunil Kumar, Arvind Yadav, N. Sudhakar Yadav, Diaa Salama Abd Elminaam & Deema Mohammed Alsekait. Secure cloud computing: leveraging GNN and leader K-means for intrusion detection optimization. Scientific Reports | (2024) 14:30906

[48] Soni, D. & Kumar, N. Machine learning techniques in emerging cloud computing integrated paradigms: A survey and taxonomy. J. Netw. Comput. Appl. 205, 103419 (2022).

[49] A. Ramachandran P. Ramadevi, Ahmed Alkhayyat and Yousif Kerrar Yousif., Blockchain and Data Integrity Authentication Technique for Secure Cloud Environment. IASC, 2023, vol.36, no.2

[50] TAN Shuang, TAN Lin, LI Xiaoling, JIA Yan. An Efficient Method for Checking the Integrity of Data in the Cloud. China Communications, September 2014

[51] ATENIESE G, BURNS R, CURTMOLA R, et al. Remote data checking using provable data possession. ACM Transactions on Information and System Security (TISSEC), 2011,14(1): 1-34.

[52] WANG Q, WANG C, LI J, et al. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems. 2011. 22(5): 847-859.

[53] A. Badhan, P. Arora, R. Garg and R. Kaur, "Energy Efficient Cloud Computing: Strategies for Reducing Data Center Power Consumption," 2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2025, pp. 1156-1162, doi: 10.1109/ICAISS61471.2025.11041956.

[54] Muthyalac, S., & Reddy, P. (2022b). Ai-Driven Cloud Access Control and Authorization Using Attribute-Based Encryption Ai-Driven Cloud Access Control and Authorization Using Attribute-Based Encryption. International Journal of Engineering Trends and Applications.

[55] Abdel-Basset M, Mohamed M, Chang V. NMCDA: a framework for evaluating cloud computing services. Futur Gener Comput Syst. 2018; 86: 12-29.

[56] Rathore S, Kwon BW, Park JH. BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network. J Netw Comput. Appl. 2019, 143: 167-177.

[57] Abdulmohsen Almalawi, Shabbir Hassan, Adil Fahad and Asif Irshad Khan., A Hybrid Cryptographic Mechanism for Secure Data Transmission in Edge AI Networks. International Journal of Computational Intelligence Systems (2024).

[58] M. A. . Omer, A. A. . Yazdeen, H. S. . Malallah, and L. M. . Abdulrahman, “A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges”, JASTT, vol. 3, no. 02, pp. 101–111, Dec. 2022, doi: 10.38094/jastt301137

[59] L. M. . Abdulrahman, S. H. . Ahmed, Z. N. . Rashid, Y. S. . Jghef, T. M. . Ghazi, and U. H. . Jader, “Web Phishing Detection Using Web Crawling, Cloud Infrastructure and Deep Learning Framework”, JASTT, vol. 4, no. 01, pp. 54–71, Mar. 2023, doi: 10.38094/jastt401144.

[60] V. Shakir and A. Mohsin, “A Comparative Analysis of Intrusion Detection Systems: Leveraging Classification Algorithms and Feature Selection Techniques”, JASTT, vol. 5, no. 01, pp. 34–45, May 2024, doi: 10.38094/jastt501186..