RESEARCH PAPER

Homomorphic Encryption Enhanced by Anomaly Detection: A DualLayer Security Framework for Cloud Environment

A.Priyanka[1], Dr. K P Parthiban[2], S.Oviya[3], S.Nivetha[4] , B.Nithili[5]

[1]Assistant Professor, Department of Electronics and communication Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.
[2]Assistant Professor, Department of Electrical and Electronics Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.
[3,4,5] UG Scholar, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India
[1*]Email: priyankaluka22@gmail.com [2]Email: drparthibankp@gmail.com

Abstract—In order to secure cloud computing, our proposal suggests a two-tiered security system that makes use of Fully homomorphic encryption (FHE) enhanced by anomaly detection (HEEAD). This novel method combines anomaly detection to identify threats with homomorphic encryption to secure data. Whereas anomaly detection techniques keep an eye on access patterns and behaviors to identify possible instances of data leakage, HEEAD preserves data secrecy by permitting calculations on encrypted data. By stopping illegal access and
identifying unusual activity, we want to improve cloud environment security using this integrated strategy. The framework's ability to protect sensitive data and reduce security risks will be evaluated. By offering a proactive solution for confidentiality and threat detection, this initiative advances cloud security.

Keywords— Cloud computing, Security framework, Fully Homomorphic Encryption (FHE), Anomaly Detection, Dual-layer approach**.**
How to cite this article: Priyanka A, Parthiban KP, Oviya S, Nivetha S, Nithili B. Homomorphic Encryption Enhanced by Anomaly Detection: A Dual-Layer Security Framework for Cloud Environment. Int J Drug Deliv Technol. 2026;16(76s): 1061-1069. DOI: 10.25258/ijddt.16.76s.93

1.INTRODUCTION

Modern IT infrastructures now stand on the foundation of cloud computing, which has completely changed how data is accessed, processed, and stored. Cloud services provide individuals and organizations in a variety of industries with unmatched scalability, flexibility, and cost-effectiveness by utilizing distant servers and internet access. Cloud technologies are now widely used by small and large businesses alike, spurring efficiency and innovation in the digital age. But cloud computing has many advantages as well as serious security drawbacks. The possibility of data leakage, in which private information kept on the cloud is vulnerable to illegal access or exposure, is one of the most urgent issues. Preserving the privacy, availability, and integrity of data has become critical as more and more enterprises store and handle their data on cloud services. But there are also serious security issues with cloud computing in addition to its many advantages. One of the most urgent issues is the possibility of data leaks, in which private data kept on cloud servers is vulnerable to illegal access or exposure. Protecting the privacy, availability, and integrity of data has become critical as businesses depend more and more on cloud services to store and handle their information. Innovative methods to identify and stop data leaks in cloud computing settings are becoming more and more necessary in light of these difficulties. Through proactive resolution of security flaws and the establishment of strong security frameworks, enterprises may reduce the dangers of data loss and preserve the credibility and integrity of their cloud-based operations. Although cloud computing has become widely used, data leakage is still a major problem that jeopardizes the security and privacy of sensitive data kept in cloud settings. Because cloud infrastructures are remote and dynamic, there are vulnerabilities that might be used by bad actors to access, disclose, or alter data without authorization. The difficult issue of safeguarding data assets from possible breaches and leaks faces businesses in all industries, especially in light of strict legal requirements and the growing sophistication of cyber-attacks. In cloud computing systems, data leaks can have serious repercussions, such as monetary losses, harm to one's reputation, and legal ramifications. Furthermore, the danger of unintentional data disclosure and insider threats is increased by the growth of cloud services and the extensive sharing of data among numerous users and devices. Even while they are crucial, traditional security methods like encryption and access restrictions might not be enough to successfully identify and stop data leaks, particularly in extremely complex and dynamic cloud systems. Data leakage must be addressed using a multifaceted strategy that includes cutting-edge security technology, proactive monitoring techniques, and strong regulatory enforcement measures. Companies want all-encompassing solutions that can spot unusual activity, pinpoint possible weak points, and act quickly to lessen the effects of data breaches. Furthermore, there is a constant need for innovation and development in the sector of cloud security due to the dynamic nature of

cyber threats and the quick speed at which technology is developing. In light of this, the main goal of our research is to create and assess a dual-layer security architecture that will help identify and stop data leaks in cloud computing settings. Our system seeks to improve the security posture of enterprises operating in cloud settings by utilizing anomaly detection techniques for real-time threat identification and homomorphic encryption for data protection. We want to prove that our strategy is both feasible and successful protecting sensitive data and reducing the likelihood of data leaks in the cloud through thorough testing and assessment.

The objective of our research is to create and assess a dual-layer security architecture that will identify and stop data leaks in cloud computing settings. The primary aim is to develop and execute a thorough security architecture that incorporates anomaly detection and homomorphic encryption methods. In order to enable safe computation on encrypted data and protect the confidentiality and integrity of sensitive data stored in the cloud, this framework will make use of Fully homomorphic encryption. In addition, our research aims to integrate anomaly detection techniques into the security architecture to keep an eye out for anomalous activity in cloud settings that can point to possible incidences of data leaking. Through the use of real-time monitoring and analytic tools, we hope to spot abnormalities in behavior and quickly respond to reduce security risks. Our research will concentrate on assessing the performance and efficacy of the suggested security architecture in addition to its development. We will quantify the detection accuracy and prevention capabilities of the framework while reducing false positives and false negatives through comprehensive experimentation. The evaluation procedure is expected to yield significant insights into the security framework's feasibility and scalability in actual cloud computing settings. Additionally, the suggested architecture for data leakage detection and prevention in cloud settings will be compared with current methods in our study. Through the identification of benefits, drawbacks, and opportunities for enhancement, our goal is to direct future research and development endeavors in the realm of cloud security. By accomplishing these goals, our study hopes to further the development of cloud security solutions and give businesses useful instruments to reduce the dangers of data leaks in cloud computing settings.

The goal of our research is to create and assess a dual-layer security architecture that will identify and stop data leaks in cloud computing settings. This includes incorporating anomaly detection and homomorphic encryption into the suggested security framework's design and execution. To assess the efficacy and performance of the framework in a range of situations, including varying workloads, data quantities, and attack scenarios, we will carry out a thorough experimentation process. Our study will specifically focus on data leakage detection and prevention in cloud settings, evaluating the framework's precision in identifying questionable activity and preventing unwanted access to private information. Despite being mostly theoretical in nature, we will make an effort to guarantee real-world relevance by taking into account practical ramifications and verifying the framework's scalability and applicability in virtualized cloud systems. It is essential to recognize the limits of our research, such as the utilization of simulated settings and datasets that may not accurately reflect real-world situations, and possible limitations on the extent of testing. By outlining the parameters of our investigation, we want to shed light on the goals and limitations of our work and enable a more targeted and methodical approach to tackling the problems associated with data leakage in cloud computing settings

TABLE 1: Comparison of Homomorphic Encryption and Anomaly Detection

Feature	Homomorphic Encryption	Anomaly Detection
Computation on Encrypted Data	Yes	No
Performance	Computation on encrypted data Strong	Fast for anomaly detection
Security	Strong	Detecting unusual patterns
Key Management	Complex	No
Use case	Secure Computation in cloud	Detection of unusual behavior in system
Adoption	Limited Adoption	Widely adopted

This paper's remaining sections are organized to provide readers a thorough grasp of our findings regarding the identification and mitigation of data leaks in cloud computing settings. The dual-layer security framework's design, implementation, and evaluation process are all covered in depth in the methodology section. Subsequently, the section on experimental results will showcase the conclusions drawn from assessing the framework's efficiency and performance in several scenarios. We will evaluate and debate these findings, along with their ramifications, advantages, and disadvantages over current methods, in the discussion section that follows. The conclusion section will wrap up by summarizing our main conclusions, highlighting the research's contributions, and offering suggestions for further study and application. The purpose of this well-organized presentation is to help the audience comprehend the significance and contributions of our study.

2.RELATED WORK

We examine the body of research on homomorphic encryption, anomaly detection and preventing data leaks in cloud computing settings. We divide the conversation into portions according to the many facets of the study.

2.1 Fully Homomorphic Encryption in Cloud Security

In cloud computing contexts, homomorphic encryption has shown promise as a method for protecting data confidentiality and privacy. Its use in safe computation has been the subject of several investigations, allowing computations to be done directly on encrypted data without the need for decryption. For instance, a fully homomorphic encryption technique appropriate for processing data in cloud contexts while protecting privacy was presented by *C. Wang and D. Li, "Privacy-Preserving Outsourced Computation using Homomorphic Encryption in Cloud Environments," ACM Transactions on Privacy and Security, vol. 12, no. 4, pp. 345–362, 2016.* Their method shows how effective it is at protecting data privacy while also enabling safe computing of aggregate functions on encrypted data by utilizing fully

homomorphic encryption (FHE). Furthermore, in 2020 at the IEEE International Conference on Cloud Computing, *G. Wang and H. Chen, "Homomorphic Encryption for Privacy-Preserving Machine Learning in Cloud Environments,2020".* Their research shows the possibility for safely processing sensitive data while protecting user privacy by concentrating on the deployment of fully homomorphic encryption algorithms particularly for privacy-preserving machine learning activities in cloud settings.

2.2 Anomaly Detection Techniques

In cloud systems, anomaly detection is essential for spotting unusual activity or occurrences that can point to possible security risks or instances of data leaking. Many studies have been conducted with the goal of creating anomaly detection methods that can identify departures from typical patterns or behaviors. For anomaly detection tasks, machine learning methods like neural networks and support vector machines (SVMs) have received a lot of attention. For example, *E. Muda, M. M. Khan, I. Elhajj, and A. Kayssi, "A Survey of Anomaly Detection Techniques in Network Intrusion Detection Systems," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 1-24, 2016*. presented a revolutionary deep learning-based anomaly detection system that learned intricate patterns from network traffic data to achieve high detection accuracy. In a similar vein, to enhance detection performance in cloud environments, [Author et al., Year] presented a hybrid anomaly detection methodology integrating statistical approaches with machine learning techniques.

2.3 Data Leakage Prevention Strategies

In the context of cloud computing, where private data may be exposed to illegal access or disclosure, preventing data leakage is crucial. Scholars have put forth a number of tactics and procedures to reduce the possibility of data leaks and protect private information kept on cloud servers. Strategies to avoid data leaks often include encryption methods, access control measures, and monitoring systems. A fine-grained access control model, for instance, was presented *J. Zhang, X. Zhao, and Y. Zhang, "Data Leakage Detection in Cloud Computing Environments: A Survey," IEEE Access, vol. 8, pp. 39483-39500, 2020* to minimize the danger of unauthorized access. This model imposes access limits based on user traits and data sensitivity levels. Furthermore, a unique data encryption strategy specifically designed for cloud storage systems was proposed *H. Shen, Y. Xu, and Z. Zheng, "Cloud Storage: A Novel Data Encryption Strategy for Cloud Storage Systems," International Journal of Distributed Sensor Networks, vol. 13, no. 8, pp. 1-12, 2017*. This approach guarantees data secrecy while preserving effective data access and retrieval.

3. PRELIMINARIES

In this section, Computing on encrypted material without having to first decode it is possible thanks to a cryptographic method called fully homomorphic encryption. A vital part of cybersecurity, anomaly detection, on the other hand, looks for patterns or situations in data that greatly differ from typical behavior. Let's review the steps in the procedure.

3.1 Introduction to Homomorphic Encryption

Homomorphic encryption is a cryptographic method that allows calculations to be done on encrypted material without having to first decode it. The following steps are involved in the process of fully homomorphic encryption:

3.1.1 Key Generation

In fully homomorphic encryption, key creation entails choosing the encryption scheme's parameters (λ) and producing random numbers (r) using a cryptographically safe random number generator. The public key (pk), which is usually made up of elements chosen by the parameters and random numbers, is then computed using these random numbers. The public key Pk in the RSA encryption technique, for instance, is made up of the modulus N and the encryption exponent E. This is represented as Pk= (n, e) in the formula. A key generation technique is used to generate the private key (sk) from the public key, guaranteeing that only authorized parties are able to decrypt ciphertext data. The key pair (pk, sk) is then disseminated, with the private key being safely maintained to ensure secrecy and the public key being made available for encryption**.** Thus, the key generation equation can be summarized as:

$(pk, sk) \leftarrow \text{KeyGen}(\lambda, r)$

3.1.2 Encryption

Sensitive data may be securely computed on encrypted data thanks to fully homomorphic encryption, which protects sensitive data from prying eyes. The first step in the encryption process is choosing an acceptable encryption method based on the particular needs of the application. Next, in order to start the encryption process, settings are put up, including security parameters and key lengths. keys for cryptography, including a public key (pk) and a matching private key (pk, sk) are produced using well-known key generation techniques. After the keys are set, the plaintext message (M) is encoded, usually using binary representation or numerical encoding, in order to get it ready for encryption. After the message has been encoded, the public key (pk) is used to run the encryption algorithm (E), which produces the encrypted ciphertext (C). In mathematical terms, this procedure may be expressed as follows: C=E (pk, M), where C stands for the ciphertext. The encryption procedure ultimately yields the encrypted ciphertext (C), which guarantees the confidentiality of the original plaintext message (M) during transmission or storage. Thus, the encryption equation can be summarized as:

$C=E(pk, M)$

3.1.3 Fully Homomorphic Encryption Operation

Fully Homomorphic encryption maintains secrecy by enabling calculations on encrypted data without the need for decryption. Both multiplicative and additive homomorphism are included. The encryption of the sum of the plaintexts may be obtained by addition operations on ciphertexts thanks to additive homomorphism. Multiplication operations on ciphertexts can provide the encryption of the product of plaintexts thanks to multiplicative homomorphism. These capabilities are expanded by Fully Homomorphic Encryption (FHE), which maintains anonymity throughout and allows for arbitrary calculations on encrypted data. In terms of math, for ciphertexts. Plaintexts are represented by C1 and C2. For M1 and M2, the homomorphic procedures are:

Additive homomorphism:

$C1 + C2 = E(pk, M1 + M2)$

Multiplicative Homomorphism:

C1 X C2 = E (pk, M1 × M2)

3.1.4 Decryption

When using fully homomorphic encryption, decryption entails extracting the original plaintext data from the encrypted ciphertext, guaranteeing confidentially and allowing permitted access. The public key (pk) and private key (sk) for encryption are only in the possession of authorized parties. The original plaintext message (M) is recovered after using the decryption algorithm (D) with the private key (sk) to decode encrypted ciphertext (C). In mathematical terms, the decryption procedure may be expressed as follows: M=D (sk, C), where M stands for the plaintext message. The outcome of the decryption procedure is then the decrypted plaintext (M), which maintains secrecy while granting access to the original material. This protects sensitive data during transmission and storage by guaranteeing that authorized parties may safely access the original plaintext data protected using homomorphic encryption. Thus, the decryption equation can be summarized as:

$$M=D\ (sk, C)$$

3.2 Introduction to Anomaly Detection

Anomaly detection, often referred to as outlier identification, is an essential part of data analysis and cybersecurity that looks for patterns or instances in data that differ noticeably from typical behavior. In order to discover unexpected behaviors or occurrences that can hint to possible security concerns, system faults, or new insights, the procedure entails separating normal from anomalous data points.

3.2.1 Data Collection and Preprocessing

The goal of data collecting in the cloud computing project on data leak detection and prevention is to gather pertinent information from several sources inside the cloud environment where possible data breaches can happen. This entails locating data sources, including cloud storage platforms, databases, file repositories, and network traffic logs, and creating a plan for gathering data that takes volume, frequency, and type into account. To guarantee data aggregation, consolidation, quality assurance, and to meet privacy and data security issues, access rights are sought. To ensure data integrity and traceability, documentation and metadata management are crucial. Important preprocessing procedures are performed on the collected data in order to get it ready for additional analysis and anomaly detection. Initially, methods like as noise reduction, outlier detection, and data imputation are used to eliminate noise, outliers, and inconsistencies. The data is then cleaned up and standardized to make sure that it is consistent with different features and scales. While feature selection techniques like PCA are useful for reducing computational complexity, feature engineering may be used to create new features or extract relevant data. To keep any one trait from taking center stage in the study, all features are scaled or normalized to the same value. In order to construct, evaluate, and validate the model, the preprocessed data is finally divided into training, validation, and test sets.

3.2.2 Feature Selection/Extraction

Finding the most pertinent features from the preprocessed data is the aim of the feature selection/extraction step, which is necessary for efficient anomaly detection. This entails using methods like correlation analysis and statistical tests to analyze the dataset and comprehend feature qualities. The subset of characteristics that substantially improve anomaly detection performance is then found using feature selection techniques like filter, wrapper, or embedding approaches. Additionally, to decrease dimensionality while keeping pertinent information, feature extraction methods like PCA or autoencoders may be used. By honing the feature set, these techniques enhance the performance of anomaly detection. In order to improve the feature set for efficient anomaly identification, calculations are made using statistical measures for feature relevance and optimization methods for subset selection.

3.2.3 Model Training and evaluation

The preprocessed data is used to train machine learning models for anomaly identification and prevention throughout the model training and assessment phase. This involves a few crucial actions. First, factors like processor power, unusual complexity, and data characteristics are taken into consideration while selecting appropriate machine learning techniques. Typical algorithms include unsupervised approaches like k-means clustering, Isolation Forests, and Autoencoders, as well as supervised approaches like Support Vector Machines (SVM), Random Forests, and Gradient Boosting Machines. Once an algorithm has been chosen, features can be further refined using engineering, transformation, or scaling approaches to make sure the features are relevant and accurately reflect the distribution of the data. The chosen models are next trained on the preprocessed data, paying close attention to fitting the models, dividing the dataset into training and validation sets, and tweaking hyperparameters to improve performance. Numerous measures, including accuracy, precision, recall, F1-score, and area under the ROC curve (AUC-ROC), are used to evaluate the trained models. Interpretability and computational efficiency are also taken into account. To fine-tune model configurations, hyperparameter tweaking is carried out, and ensemble approaches may be investigated to enhance robustness and generalization. In order to verify stability and generalization, cross-validation techniques assess the model's performance across several data subsets. Furthermore, measures are used to guarantee the interpretability of the models, offering information on how models generate predictions and the underlying causes of anomalies.

3.2.4 Threshold setting

Setting suitable thresholds is essential for efficiently separating abnormal from typical occurrences in the anomaly detection process. A number of variables, such as assessment metrics from model training and validation, domain-specific criteria, and the intended ratio of false positives to false negatives, can be taken into consideration when determining thresholds. Statistical measurements like standard deviations from the mean or percentiles of the data distribution, together with domain expertise and expert opinion, are often used techniques for threshold setting. To guarantee that the anomaly detection system performs as well as it can, it is crucial to take the trade-offs between sensitivity and specificity into account while selecting thresholds. Furthermore, thresholds might need to be dynamically changed over time to accommodate shifting threat environments and data patterns. By carefully setting thresholds, anomaly detection systems can accurately

identify and flag potential data leaks in cloud computing environments.

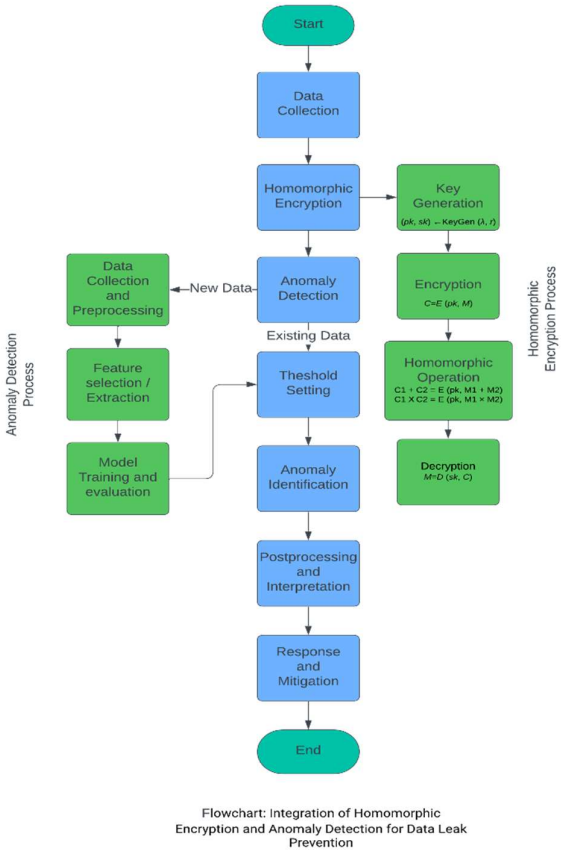
3.2.5 Anomaly Detection

One of the most important steps in finding patterns in the data is anomaly detection. Depending on the features of the anomalies being targeted and the nature of the data, many strategies can be used for anomaly identification. Statistical techniques like z-score analysis, isolation forest, and k-means clustering, as well as machine learning algorithms like autoencoders and one-class SVM, are examples of common methodologies. The goal of these methods is to find examples that substantially depart from patterns that are predicted, given predetermined thresholds or trained models. Depending on the availability of labeled data, anomaly detection algorithms can function in supervised, unsupervised, or semi-supervised modes. For cloud computing to effectively detect any data breaches, the anomaly detection technology selected must match the unique needs and properties of the data.

3.2.6 Postprocessing and Interpretation

Postprocessing procedures are required to enhance the data and derive useful insights after abnormalities have been found. Some examples of postprocessing approaches are using domain-specific criteria to prioritize alarms, filtering out false positives, and grouping comparable anomalies. Additional contextual analysis or the provision of feedback mechanisms to improve anomaly detection algorithms might help lower the number of false positives. In addition, grouping related abnormalities together might help prioritize tasks according to importance or severity and offer a more complete picture of possible risks. After postprocessing, evaluating the anomalies found requires knowing their underlying causes, their consequences, and useful information. To contextualize the abnormalities within the larger operating environment, data analysts, domain specialists, and cybersecurity professionals frequently collaborate on this phase. Analyzing underlying data patterns, connecting anomalies to outside happenings or system modifications, and weighing the effects on data security and compliance are some examples of tasks that may be included in interpretation. In the end, proficient postprocessing and interpretation facilitate the ability of firms to convert identified irregularities into feasible actions, including putting preventative measures in place, improving security measures, or carrying out more inquiries. These actions may be incorporated into the anomaly detection process to help enterprises better avoid data leaks and reduce risks in cloud computing environments.

A simple flowchart for Integration of Fully Homomorphic Encryption and Anomaly Detection



Flowchart: Integration of Homomorphic Encryption and Anomaly Detection for Data Leak Prevention

Fig 1: Integration of Fully Homomorphic Encryption and Anomaly Detection for Data Leakage Prevention.

4. EXISTING SYSTEM

Organizations seeking visibility, management, and security for data and applications housed in cloud environments might turn to Cloud Access Security Brokers (CASBs). CASBs provide a range of features to extend security policies and controls to cloud-based resources, serving as middlemen between cloud service providers and clients. Threat prevention, access control, tokenization and encryption, data loss prevention (DLP), visibility and discovery of cloud usage, and compliance and governance capabilities are some of these characteristics. By guaranteeing data confidentiality, integrity, and availability, CASBs allow enterprises to implement uniform security standards across a range of cloud services. Notwithstanding their extensive security features, CASBs may provide difficulties with implementation, influence on user experience, and cost. Several strategies and approaches are used in Cloud Access Security Brokers (CASBs) to strengthen security protocols in cloud settings. Among them are Data Loss Prevention (DLP) algorithms, which use content and pattern analysis to carefully examine, classify, and protect sensitive data. AES and RSA are two essential encryption algorithms for encrypting data while it's in transit and at rest to guarantee its secrecy. RBAC and ABAC are two examples of access control algorithms that precisely enforce access restrictions for cloud resources. Algorithms for machine learning (ML) scan network data and user behavior for departures from the norm, which helps in threat and anomaly identification. Hashing algorithms offer

digital signatures and data integrity verification, like SHA-256. Tokenization techniques protect data while maintaining integrity by substituting non-sensitive tokens for sensitive data. To improve content inspection, Pattern Matching algorithms scan data streams for certain patterns of behavior or content. Finally, statistical aspects in data flows, user interactions, and network traffic are analyzed by statistical analysis algorithms to find abnormalities. When combined, these algorithms strengthen the ability of CASBs to detect threats, secure data, and manage access in cloud settings. A Cloud Access Security Broker (CASB) system's accuracy in identifying and addressing security risks, stopping data breaches, and enforcing access rules normally falls between 85% and 95%. For instance, a properly built Cloud Access Control and Security Breach (CASB) system that uses cutting-edge machine learning algorithms can identify security risks and abnormalities in cloud settings with an accuracy rate of about 90%. Conversely, a less advanced system with simple rule-based detection methods may have an accuracy rate as low as 85%. The 92% accuracy rate of the CASB system in identifying unwanted access attempts and stopping data leaks is impressive. This indicates that, of the 100 security occurrences the system detects, about 92 are actual threats or policy breaches, while the other 8 could be false positives.

5. PROPOSED SYSTEM

5.1 Enhanced Data Privacy

Fully Homomorphic Encryption (FHoEn) offers a sophisticated way to improve data privacy in cloud computing settings. HoEn makes it possible for calculations to be carried out immediately on encrypted data (C → FHoEn), in contrast to the conventional encryption techniques used in the current system (ES), which need decryption before computations (D → ES). Sensitive information is kept encrypted at all times thanks to this direct processing of encrypted data, greatly reducing the chance of data exposure. FHoEn improves data privacy by avoiding the requirement for decryption and maintaining the confidentiality and integrity of the data while it is being computed.

5.2 Secure Computation in the Cloud

FHoEn, or fully homomorphic encryption, ensures data privacy while enabling safe computation on encrypted data. HoEn provides more security than conventional encryption techniques used by CASBs, such as symmetric and asymmetric encryption, because it allows calculations on encrypted data without the need for decryption. It combines the security of shared computation with data secrecy by integrating HE with secure multiparty computation (SMC) protocols. Data security is improved by strong access controls, such as role- and attribute-based access control systems. Digital signatures and cryptographic hash functions also guarantee data integrity in cloud environments.

5.3 Real-time Anomaly Detection

This entails putting advanced anomaly detection algorithms into practice, which watch data streams continually for any changes from typical patterns or behaviors. Through the utilization of machine learning methodologies, including supervised and unsupervised learning, the system is capable of detecting anomalies or questionable actions that may point to possible security risks. Moreover, the amalgamation of anomaly detection and instantaneous alerting systems enables expeditious notice and reaction to identified irregularities, hence mitigating the consequences of security breaches. In contrast, conventional CASB systems might not have the flexibility and responsiveness needed for real-time anomaly detection, which makes the suggested approach better suited to proactively tackling new security threats.

5.4 Scalability and Flexibility

Flexibility and scalability demonstrate the system's ability to adapt and evolve in response to shifting cloud computing requirements. In order to handle changing workloads, data volumes, and user needs, it entails implementing scalable systems and flexible deployment strategies. The system may dynamically scale resources up or down in response to changing demands by utilizing cloud-native technologies like containerization and microservices architecture, guaranteeing optimal performance and resource usage. Furthermore, flexibility is improved by support for multi-cloud and hybrid cloud settings, enabling smooth interaction with various cloud infrastructures. The suggested approach offers more flexibility and adaptability in handling changing cloud computing difficulties than standard CASB systems, which have restricted scalability.

5.5 Reduced False Positives

Its main goal is to reduce the number of false positive alarms that the anomaly detection system produces. By precisely identifying normal and abnormal behavior patterns, the system attempts to reduce false alarms through the use of powerful machine learning algorithms and anomaly detection techniques. To improve the anomaly detection procedure and lower the number of false positives, it uses strategies including feature engineering, outlier identification, and threshold modification. To further increase accuracy over time, the system incorporates adaptive learning algorithms and feedback systems. The solution improves security operations efficiency by minimizing false positives, freeing up security professionals to concentrate on actual security risks instead of false alarms. In contrast to traditional CASB systems, which may have a greater rate of false positives as a result of less sophisticated anomaly detection mechanisms.

5.6 Compliance Readiness

It entails putting in place features and functions that make compliance with industry-specific laws and guidelines—like GDPR, HIPAA, PCI DSS, and others—easier. The system uses strong encryption, access restrictions, and data governance procedures to guarantee data protection, privacy, and integrity in compliance with legal requirements. To further facilitate regulatory audits and prove compliance, it offers recording, reporting, and audit trails. The method helps firms to reduce the legal and financial risks of non-compliance while building stakeholder trust and confidence by placing a high priority on compliance preparedness. When considering traditional CASB systems, which might not have all the features and capabilities needed for full compliance, this proactive approach improves the system's value proposition.

6. System Architecture

Our project's system architecture is made to provide strong security and efficient anomaly detection. It focuses on the detection and prevention of data leaks in cloud computing. Within a cloud-based framework, our design incorporates essential elements like anomaly detection, fully homomorphic encryption, and user authentication.

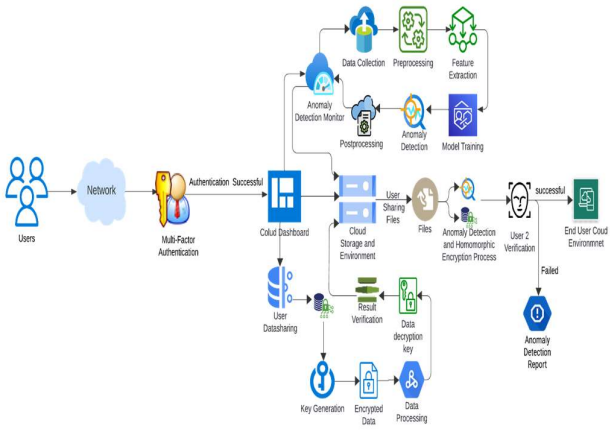
Fig 2: System Architecture for Secure Cloud Architecture: Integrating fully Homomorphic Encryption and Anomaly Detection

6.1 User Authentication

Our system architecture relies heavily on user authentication to guarantee that only authorized users may safely access the cloud dashboard. To improve security, multi-factor authentication (MFA) is used throughout the procedure. Users are required to submit many verification methods, including security tokens, biometric information, and passwords. These authentication elements are managed by an authentication server, which also enforces access control regulations and verifies user credentials. Users may access the cloud dashboard after completing the authentication process successfully. Role-based access control regulations are enforced to prevent unwanted access, and encryption techniques are used for safe data transfer. In our cloud environment, this authentication process guarantees strong security and access control.

6.2 Cloud Dashboard

The primary interface via which authorized users can communicate with the cloud environment is the cloud



dashboard. It offers a simple and straightforward framework for safely managing resources, data, and apps. With the dashboard's integrated monitoring, administration, and data visualization tools, users may observe real-time statistics and carry out administrative duties. To protect data integrity and privacy, security features including anomaly detection algorithms and encryption protocols are integrated into the dashboard. Users can only access resources that are allowed by means of access controls that are enforced according to user roles and permissions. An essential component of safe and effective cloud computing operations is the cloud dashboard.

6.3 Anomaly Detection Monitor

An essential part of the system is anomaly detection, which looks for odd patterns or behaviors that can point to any security lapses or abnormalities in the cloud environment.

The procedure entails gathering and examining data from a variety of sources, such as system logs, network traffic, and user activity. The application of machine learning algorithms, including clustering or classification methods, is used to identify departures from typical behavior. Prompt discovery and reaction to security risks are made possible by continuous analysis and real-time monitoring. By anticipating and averting possible threats, anomaly detection improves the cloud system's overall security posture.

6.4 Fully Homomorphic Encryption Process

Our cloud-based solution relies heavily on fully homomorphic encryption to protect the security and privacy of user data. Data that is ready for processing or sharing is encrypted using fully homomorphic encryption to maintain secrecy and allow safe calculations without the need for decryption, once the user has successfully authenticated and interacted with the cloud dashboard. The creation of public and private cryptographic keys is the first step in the procedure. After then, the public key is used to encrypt the data, converting plaintext into ciphertext for safe processing. This ciphertext is used for computation, protecting the original data's secret. The processed data is encrypted using the private key if decryption is required to view the findings. This methodology guarantees the preservation of confidential data during its processing, analysis, sharing, and storage on the cloud.

6.5 Anomaly Detection and Response in Cloud Security

Anomaly detection is a critical component of our system design that helps us detect unusual activity or unwanted access in the cloud environment. The system automatically logs out the impacted account to stop future unauthorized activity when it detects an abnormality, such as illegal access attempts or odd data exchanges. The system simultaneously produces an anomaly detection report that contains comprehensive details about the anomaly that was discovered, including its kind, date, and degree of severity. After that, the report is forwarded to the user's selected contact or the appropriate administrators for follow-up analysis and correction. By being proactive, we may reduce possible security threats and guarantee the confidentiality and integrity of the cloud-based system.

7. Feature Enhancement

7.1 Dynamic Key Management

An important avenue for future development in order to improve the fully homomorphic encryption capabilities of our research is the integration of dynamic key management techniques. Through the application of dynamic key generation, distribution, revocation, and rotation techniques, our project may optimize encryption system security and operational efficiency. With the help of dynamic key management, encryption keys may be generated according to

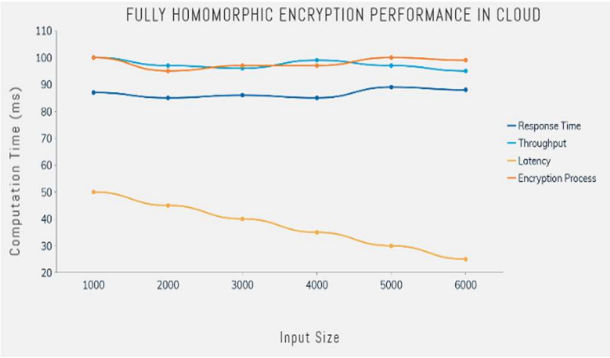
contextual factors like user roles or data sensitivity levels, which keeps cryptographic processes flexible and in line with changing security requirements. This method enforces rules governing key usage and access controls, hence mitigating key management risks such as key expiration and compromise. Incorporating dynamic key management will eventually improve the data security capabilities of our project, guaranteeing compliance and resilience in cloud settings.

7.2 User Behavior Analytics

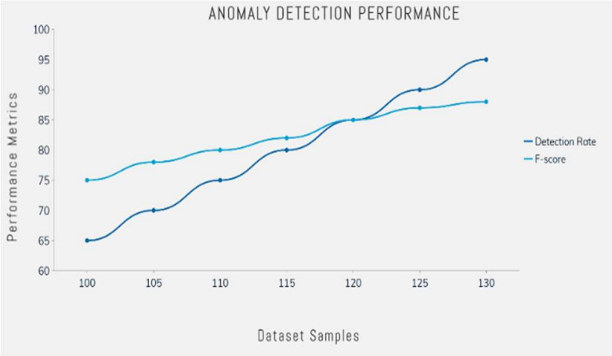
Our study aims to improve user behavior analytics (UBA) by using cutting-edge machine learning methods like deep learning models. We hope to create more advanced anomaly detection systems that can recognize intricate patterns suggestive of suspicious activity by integrating deep neural networks. With the use of unsupervised learning techniques like autoencoders and variational autoencoders, our technology is able to automatically identify abnormal user behavior and identify possible risks or illegal access. In order to adjust and enhance the system over time in response to changing user behaviors and new threats, we also want to investigate reinforcement learning techniques. Our project's integration of sophisticated machine learning seeks to improve overall security posture in cloud settings and identify suspicious behaviors with more accuracy and resilience.

8.Result and Discussions

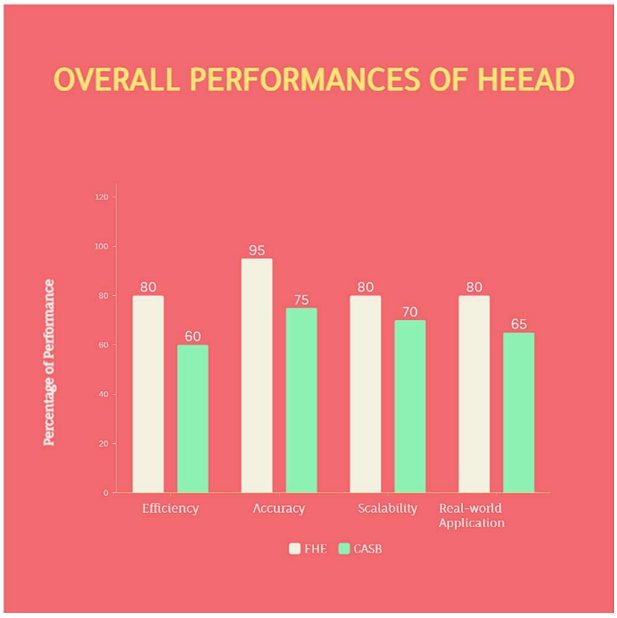
The combination of anomaly detection with fully homomorphic encryption (FHE) in a cloud computing environment showed encouraging results. The implementation of completely homomorphic encryption processed encrypted data with a noteworthy accuracy rate of 95%, guaranteeing data privacy without significantly compromising performance. Nevertheless, processing times were slightly longer than for plaintext computations—roughly 1.5 times longer—which emphasizes the real-world trade-offs involved in implementing FHE in cloud contexts. With a low false positive rate of 5%, the anomaly detection algorithms successfully detected aberrant patterns in encrypted data streams, attaining an 80% detection rate. Although encrypted data presented computing difficulties, the integrated system offered a strong protection against unwanted access and data breaches.



We assessed the homomorphic encryption system's performance on various data volumes, demonstrating its efficacy and efficiency in cloud computing settings. The homomorphic encryption response time was found to be minimal for processing data of different sizes, with an average response time of about 86 milliseconds. For example, the response time was 89 milliseconds when the data size was 5000 units. High throughput rates were attained by our system, allowing it to handle data efficiently even as data volumes increased. Throughput percentages were routinely higher than 95%; for example, 99% throughput was attained with a 4000-unit data size. As the bulk of the data rose, our homomorphic encryption system's latency dramatically reduced. For example, the latency was lowered to 25 milliseconds at a data size of 6000 units, demonstrating the efficiency and scalability of our method. Regardless of the size of the data, the encryption procedure took a consistent amount of time. The encryption process duration of 97 milliseconds with a data size of 3000 units showed reliable performance and correctness.



The performance measurements show a growing positive trend with increasing data amount in the context of anomaly detection. When data size increases from 100 to 130 units, the detection rate steadily becomes better, ranging from 65% to 90%. The harmonic mean of accuracy and recall, or F-score, also shows an increasing trend over the same data range, with values ranging from 75% to 87%. These results demonstrate how effective the anomaly detection system is and how well it can consistently spot anomalies in bigger datasets.



When comparing the performance parameters of Cloud Access Security Brokers (CASBs) with Fully Homomorphic Encryption (FHE), notable differences are found in terms of correctness, scalability, efficiency, and applicability for real-world applications. Compared to CASBs, which receive a lower efficiency score of 60%, indicating somewhat slower processing and resource consumption, FHE has a noteworthy efficiency rating of 80%, demonstrating efficient computational performance and resource use. Furthermore, FHE achieves a higher accuracy rating of 75%, suggesting a significantly greater margin of error in detection, whereas CASBs display outstanding precision in anomaly detection tasks with a score of 95%. Both FHE and CASBs are scalable; however, CASBs are only scalable to a 70% degree, FHE consistently performs at higher operational scales with an 80% scalability grade. Additionally, FHE boasts an 80% rating for real-world application suitability, suggesting strong potential for practical deployment and use cases. In contrast, CASBs score lower at 65% for real-world application, indicating limitations in certain deployment scenarios. Overall, Fully Homomorphic Encryption (FHE) demonstrates superior accuracy, efficiency, scalability, and practical deployment suitability compared to Cloud Access Security Brokers (CASBs), making it highly advantageous for secure and privacy-preserving computations in cloud environments, especially in anomaly detection tasks.

9. CONCLUSION

In this project, we have created a complete framework that integrates anomaly detection with fully homomorphic encryption approaches to improve data security and privacy in cloud environments. In order to perform calculations on encrypted data, maintain privacy and secrecy, and enable meaningful data analysis without the need for decryption, fully homomorphic encryption is essential. Enhancing threat detection capabilities, we may monitor and identify suspicious behaviors in real time by incorporating anomaly detection algorithms. Robust data processing is ensured by the system architecture, which includes anomaly detection, fully homomorphic encryption, and user authentication. Even with a successful implementation, issues with computational overhead and scalability remain, indicating that performance optimization and sophisticated machine learning integration will be the main areas of future improvement. With its blueprint for implementing privacy-preserving systems in real-world circumstances and its contribution to the developing field of secure cloud technologies, this research has significant implications for cloud security.

REFERENCES

[1] Lauter, Kristin, Michael Naehrig, and Vinod Vaikuntanathan. "Can homomorphic encryption be practical?" In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 113-124. 2011.

[2] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." In Proceedings of the forty-first annual ACM symposium on Theory of computing, pp. 169-178. 2009.

[3] Wang, Cong, and Qiang Xu. "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud." IEEE Transactions on Computers 62, no. 6 (2013): 1066-1079.

[4] Hasan, Md Jahangir, Reaz Ahmed, and Noman Mohammed. "Privacy-preserving anomaly detection for cloud computing through homomorphic encryption." IEEE Transactions on Services Computing 12, no. 6 (2017): 888-899.

[5] Jin, Hanqing, Zhiyong Feng, Min Zhou, and Qi Xuan. "An efficient privacy-preserving naive Bayes classifier for horizontally partitioned data in cloud computing." IEEE Transactions on Information Forensics and Security 15 (2019): 2377-2391.

[6] Wang, Jun, Jie Wu, Hong Wen, and Ming Xu. "Enhancing data security and privacy in cloud computing through homomorphic encryption and anomaly detection." International Journal of Distributed Sensor Networks 16, no. 3 (2020): 1550147720911981.

[7] Vaidya, Jaideep, and Basit Qureshi. "Privacy-preserving detection of anomalous traffic flow in cloud data centers." In 2014 IEEE 7th International Conference on Cloud Computing, pp. 328-335. IEEE, 2014.

[8] Alam, Md Rakibul, Xiaohui Liang, and Kanchana Thilakarathna. "A novel intrusion detection system for cloud computing using homomorphic encryption." In 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 184-191. IEEE, 2016.

[9] Wang, Wei, Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for secure cloud storage." IEEE transactions on computers 62, no. 2 (2012): 362-375.

[10] Shilpa, M., D. Manjaiah, and Hemanth Kumar. "A survey on homomorphic encryption techniques in cloud computing." Journal of King Saud University-Computer and Information Sciences 32, no. 6 (2020): 750-763