Application of Machine Learning Algorithms with Zero Trust Principles for Preventing Malware and SQL Injection Attack in a Cloud Database

Obasi E.C.M.
Department of Computer Science and Informatics,
Federal University, Otuoke, Bayelsa State
https://orcid.org/0009-0001-1513-9887

Timadi M.E.
Department of Computer Science and Informatics,
Federal University, Otuoke, Bayelsa State
https://orcid.org/0009-0002-4419-2385

ABSTRACT

Cloud databases face persistent threats such as SQL injection and malware attacks that compromise confidentiality, integrity, and availability. This study proposes a Zero Trust Cloud Database Access Control system that integrates supervised machine learning and encryption to provide robust security. The framework enforces continuous verification by subjecting every query and file upload to real-time inspection, regardless of prior authentication. A Feedforward Neural Network (FFNN) was employed to classify SQL queries as benign or malicious, achieving 98% accuracy with high precision in detecting SQL injection attempts. In parallel, a Random Forest classifier was used for malware traffic detection, attaining 99.37% accuracy by analyzing behavioral and statistical features. The system further incorporates encryption mechanisms to secure sensitive information, ensuring that only authorized users with valid keys can access decrypted data. Results demonstrate that combining zero-trust principles with advanced machine learning significantly strengthens defense against evolving threats, reduces false positives, and maintains data confidentiality. The modular design and adaptability of the framework make it suitable for addressing emerging challenges in cloud database security.

General Terms

Security, Cloud Computing, Machine Learning, Behavioral Analytics, Zero Trust Architecture, Algorithms

Keywords

Cloud Database Security, SQL Injection Detection, Malware Detection, Zero Trust Access Control, Feedforward Neural Network (FFNN), Random Forest Classifier, Data Encryption, Anomaly Detection.

1. INTRODUCTION

Data security is a fundamental aspect of modern information systems, involving the protection of digital information from unauthorized access, corruption, or theft throughout its lifecycle. It spans hardware, software, managerial, and access control measures designed to safeguard organizational data assets against cybercriminal activities, insider threats, and human error [3]. The increasing reliance on cloud computing for data storage and online services has introduced new security challenges, particularly in cloud databases. While cloud platforms provide scalability, flexibility, and accessibility, they also expose data to vulnerabilities such as SQL injection, malware, and distributed denial-of-service (DDoS) attacks [6] [29].

Traditional perimeter-based security models are increasingly inadequate for protecting cloud-hosted databases due to their distributed and dynamic nature. As a result, the Zero Trust Architecture (ZTA) has emerged as a promising paradigm. Unlike conventional security approaches, zero trust assumes that no user, device, or network can be inherently trusted, regardless of location or previous access privileges [22]. In this model, every access attempt undergoes continuous authentication, authorization, and monitoring, thereby reducing risks from both external and insider threats.

To further enhance cloud database security, researchers are integrating machine learning (ML) algorithms and behavioral analytics into access control mechanisms. ML models can analyze large-scale data streams in real-time to detect malware, anomalous queries, and SQL injection attacks with high accuracy [32][24]. Behavioral analytics complements this by profiling user activity to establish normal patterns and identify anomalies such as unusual access times, irregular query volumes, or attempts to access sensitive records [12]. Together, these techniques improve proactive threat detection and response in cloud environments.

Despite the advantages, significant challenges remain. One limitation is the scarcity of high-quality, unbiased datasets for training and validating ML classifiers. Privacy concerns and the restricted availability of internal datasets hinder progress, forcing researchers to rely on synthetic or benchmark datasets such as UNSW and ISOT [9]. Additionally, advanced malware can evade traditional detection systems, highlighting the need for trusted frameworks capable of addressing evolving and unknown threats.

This study proposes a Zero Trust Cloud Database Access Control framework that combines supervised ML algorithms with behavioral analytics and encryption. By adopting a multi-layered approach, the framework aims to provide comprehensive protection against SQL injection and malware attacks, ensure confidentiality of sensitive data, and enhance organizational resilience against cyber threats.

2. REVIEW OF RELATED LITERATURE

2.1. Cloud Computing and its Challenges

Cloud computing has revolutionized data storage and management by offering scalable, flexible, and cost-efficient solutions through cloud databases [16]. One of the main challenges in cloud computing is security. The shift from traditional IT infrastructure to cloud-based solutions introduces new security and privacy concerns. Data breaches and unauthorized access are significant threats that can undermine user trust and data integrity [14]. Security issues arise due to the cloud's inherent characteristics such as multi-tenancy and elasticity, as well as the third-party control over data, leading to vulnerabilities in confidentiality, integrity, availability, and trust [27]. Another critical concern is data privacy. As businesses increasingly rely on cloud services, protecting personal and sensitive information becomes paramount. This involves ensuring compliance with regulations and maintaining rigorous data protection mechanisms to prevent unauthorized data dissemination [23]. Moreover, the dynamic nature of cloud services necessitates robust security frameworks capable of evolving with emerging threats [11]. The increasing adoption of cloud computing for storing sensitive information and providing online services has led to a growing need for robust security measures to protect against cyber-attacks, particularly malware and SQL injection attacks. Traditional signature-based detection methods are becoming ineffective against modern threats, necessitating the development of more advanced, intelligent security solutions [3][13].

A significant challenge in developing such solutions is the lack of readily available, robust datasets containing patterns and historical data to train machine learning classifiers for detecting attacks [30]. Additionally, Aboh and Janjua emphasizes that many current detection models perform well only on known attacks (i.e. those in training data), and that the evolving nature of threats means models must be evaluated more rigorously for *"novel or zero-day attacks"* .They note that AI-driven methods are increasingly used to handle *unknown or unseen threat patterns* by leveraging techniques that can generalize beyond signature-based detection [1].

Cloud databases, whether relational or non-relational, provide organizations with the advantage of accessing data anywhere and scaling dynamically without the need for physical infrastructure investment [15]. Cloud security is a set of security measures designed to protect cloud-based infrastructure, applications, and data. These safeguards protect data privacy by ensuring user and device authentication, data and resource access control, and data access control. Moreover, they also assist with keeping data compliance requirements. One of the primary concerns in cloud database security is data confidentiality and privacy during storage and transfer. Advanced Encryption Standard (AES) has been proposed as a solution to secure data transfer and storage in cloud computing environments [8]. Additionally, authentication, access control, encryption, auditing, intrusion detection, and privacy-enhancing techniques are crucial components of database security in cloud environments [21]. In essence, Cloud Database Security protects a company's data from data breaches, distributed denial of service (DDoS) attacks, viruses, hackers, and unauthorized user access or use in cloud environments. While cloud databases offer numerous advantages, they are not without their challenges. Like all technological systems, they can be vulnerable to various threats. These threats can compromise the security of the data stored within the cloud database, potentially causing significant damage to users. While cloud computing offers significant advantages, addressing its challenges is essential for widespread adoption and trust in cloud-based solutions. Researchers and practitioners are continually exploring innovative solutions to mitigate these challenges and safeguard cloud environments [26].

2.2. Machine Learning in Solving Real Life Challenges

Machine learning (ML) has become a transformative technology for solving complex, real-world problems across domains such as cybersecurity, healthcare, finance, transportation, and cloud computing. Its ability to process large-scale data, recognize hidden patterns, and adapt to evolving contexts makes it particularly effective for addressing dynamic and adversarial challenges. Many researchers have applied machine learning algorithm in solving numerous problems. Obasi and Nlerum developed a model for the Detection and Prevention of Backdoor Attacks using CNN with Federated Learning[19]. Timadi and Obasi researched on Integrating Zero-Trust Architecture with Deep Learning Algorithm to Prevent Structured Query Language Injection Attack in Cloud Database [28]. Nnodi and Obasi researched on Leveraging Artificial Intelligence for Detecting Insider Threats in Corporate Networks [17]. Obasi and Stow formulated a Predictive Model for Uncertainty Analysis Pertaining to Big Data through the Utilization of a Bayesian Convolutional Neural Network (CNN) [20]. Again, Machine learning models was applied to predict reaction yields with high accuracy, guilding chemists in selecting high-yielding reactions and optimizing synthesis routes. A research on Leveraging Machine Learning Algorithms for Enhanced Prediction of Product Yields and Purity in Chemical Reactions was developed [18]. Also, ML applications in **healthcare** illustrate its real-world impact. Predictive analytics using ML algorithms can detect diseases such as cancer and cardiovascular conditions from medical imaging and sensor data, achieving higher accuracy than manual diagnosis in certain cases [1]. To that effect, an interpretable Early Warning System for Malaria Outbreak in Bayelsa State using Deep Learning and Climate Data was developed in 2025 [25].

In **cybersecurity**, ML has advanced malware and intrusion detection beyond signature-based systems, which are limited to known attack patterns. Recent studies demonstrate that supervised, unsupervised, and meta-learning algorithms significantly improve detection accuracy, particularly for *unknown or zero-day attacks*. This shows ML's potential for real-world deployment in environments where threats evolve daily. The effectiveness of ML in detecting zero-day malware attacks, which are challenging for traditional signature-based approaches, is particularly notable. By analyzing malicious patterns, ML algorithms can accurately detect polymorphic malware, which is essential for robust cybersecurity measures [2]. Moreover, ML models have been employed to mitigate SQL injection attacks (SQLIAs), which pose significant threats to cloud-hosted web applications. Supervised learning models, such as Two-Class Support Vector Machine (TC SVM) and Two-Class Logistic Regression, have been trained to differentiate between malicious and benign web requests, achieving high accuracy in SQLIA detection [30]. The application of machine learning extends beyond simple detection; it involves feature extraction and selection to enhance detection accuracy. In SQL injection detection, various ML techniques have demonstrated a detection rate higher than 98%, leveraging classifiers trained on malicious and benign payloads [29]. Hybrid approaches, such as combining CNN (Convolutional Neural Networks) with BiLSTM (Bidirectional Long Short-Term Memory), have shown superior performance in detecting SQLI attacks, highlighting the versatility and adaptability of ML in cybersecurity scenarios [4].

2.3. Integrating ML, Encryption, with Zero Trust Principles

Integrating machine learning with encryption and zero trust principles provides a comprehensive cybersecurity framework that enhances the protection mechanisms for cloud databases. Zero trust security models emphasize the "never trust, always verify" approach, where verification is continuously re-evaluated. In this context, machine learning models play a critical role in maintaining vigilance against threats by analyzing data patterns and identifying anomalies that suggest potential security breaches. By incorporating ML with zero trust principles, it's possible to dynamically adjust security policies and enforce stricter access controls based on real-time threat intelligence.

Encryption is another critical component in this integrated system. It ensures that even if data is intercepted, it remains unreadable and secure. Machine learning algorithms can enhance encryption strategies by predicting potential vulnerabilities and adapting encryption keys and protocols accordingly. Combining these techniques ensures a robust defense against malware and SQL injection attacks, which are significant threats to cloud databases due to their potential to expose sensitive data and disrupt services [7][5].

The synergy of ML, encryption, and zero trust principles creates a multilayered security framework. This framework not only detects and prevents attacks but also proactively adapts to emerging threats and vulnerabilities. By leveraging ML's predictive capabilities, organizations can anticipate potential threats, thus enabling a preemptive approach to database security. This proactive stance is vital as cyber threats become increasingly sophisticated, necessitating more intelligent and adaptive security measures [3].

3. MATERIALS AND METHODS

This research work employs a quantitative research design, utilizing a deep learning approach to detect and prevent SQL injection attacks and Random Forest algorithm to detect and prevent sophisticated malwares attack in a cloud databases. For SQL injection attack, a labeled dataset of SQL queries, including benign and malicious queries (SQL attacks and non-SQL attacks) was obtained from an online database, Kaggle.com. The architecture of the proposed system is shown in Figure 1. Tokenization, normalization, and feature extraction were carried out after obtaining the dataset which includes SQL queries from public sources and cloud database logs. The data was pre-processed by tokenizing SQL queries, removing stop words, and converting to numerical representation. Tokenization splits SQL queries into individual words or tokens. Normalization transforms tokens into a consistent format such as lowercasing and punctuation removal. A Feed Forward Neural Network (FFNN) algorithm was used to classify SQL queries as benign or malicious (SQL attacks and non-SQL attacks). 80% of the dataset was used for training while 20% was used for testing. The model achieved a training result of about 98% and a test result of about 98%. The classification report serves as a comprehensive summary of the metrics including accuracy, precision, recall, and f-measure. Precision pertains to the accurate classification of the model as it relates to false positives, false negatives, true positives, and true negatives. The precision score of the model indicates an approximate 100% accuracy in the classification of normal queries and a 94% accuracy in the classification of queries indicative of SQL injection attacks. The model has successfully identified anomalies within database queries and signaled potential SQL injection threats. Having detected anomalies in database queries and flagged potential SQL injection attacks.

For malware detection and prevention, we used Random Forest classifier tree to classify the malware/benign files. The dataset that we used contained 70% malwares and 30% benign files. As per the splitting part, we divided the data into 80% training data and 20% testing data and then we selected the important features that are required for the classification using the extratrees.feature_importances_ function. The Accuracy percentage of Random Forest Classifier was 99.37%.

This architecture of the proposed system in figure 1 illustrates a machine learning-based cybersecurity architecture designed to detect and prevent SQL and malware attacks on a cloud database system using Zero-Trust principles. The Zero Trust Principle is a foundational security concept embedded in the architecture, ensuring robust protection for the cloud database. Unlike traditional security models that assume trust within a network perimeter, Zero Trust operates on the premise that no entity—whether inside or outside the network—should be inherently trusted. Every access request is verified continuously based on multiple contextual factors such as identity, device health, location, and behavior.

In the given architecture, Zero Trust is placed as a gatekeeper between the user's request and the cloud database. This enforcement layer ensures that every request is authenticated and authorized before being granted any level of access to the database. It does not assume that a legitimate-looking request is safe; instead, it demands proof of trustworthiness for every transaction. It also integrates encryption to ensure that sensitive data are encrypted with secret key. In the proposed system architecture, encryption plays a crucial role in ensuring data security and confidentiality during both storage and communication. This security mechanism is a vital line of defense against unauthorized data access, eavesdropping, and data breaches. Encryption is the process of converting plain data into an unreadable format (ciphertext) using cryptographic algorithms. Only authorized parties with the correct decryption key can convert it back to a readable format. Encryption protects against man-in-the-middle attacks, where attackers intercept the communication between the user and the database or model.

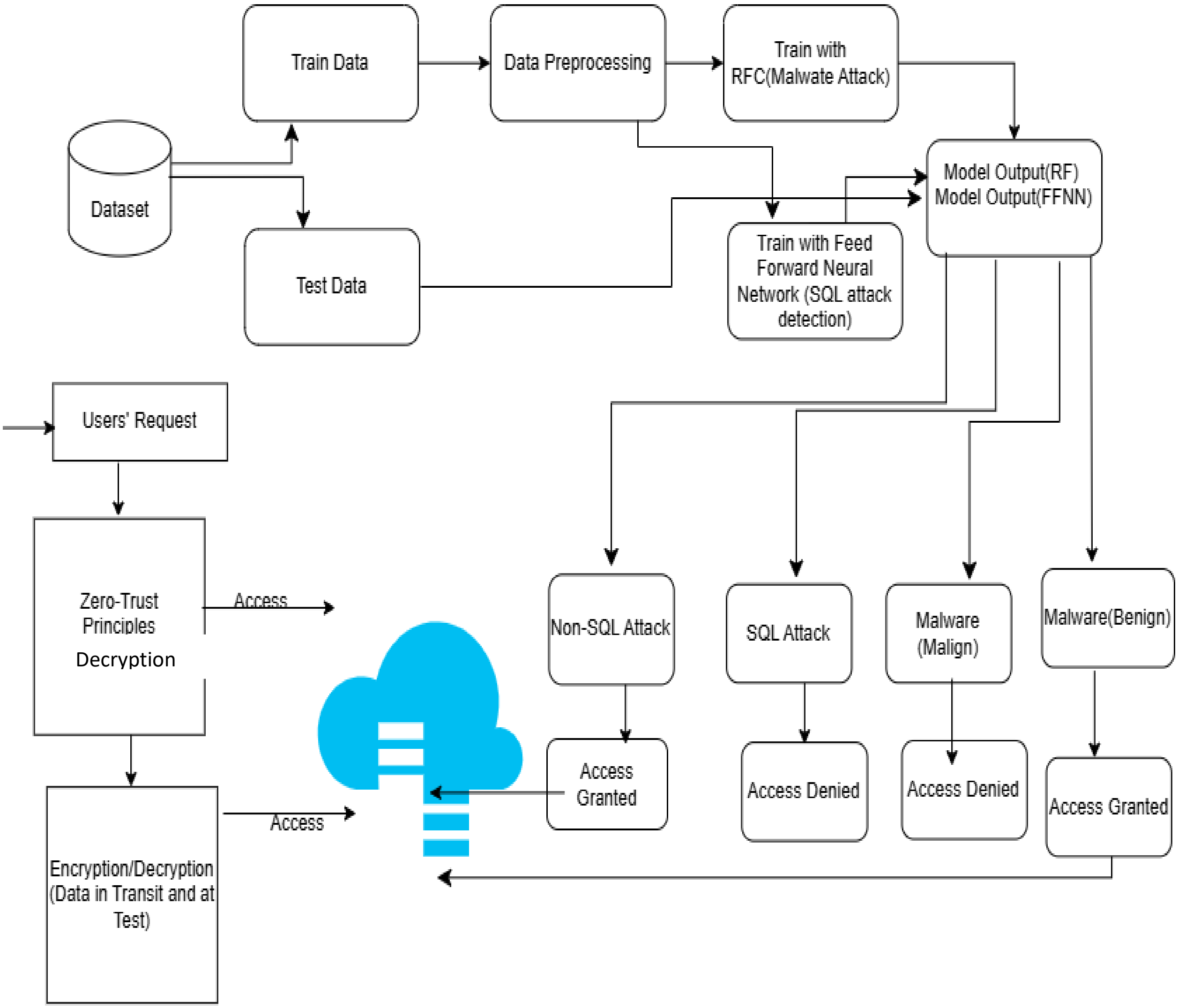


Figure 1: Architecture of the Zero Trust Cloud Database Access Control System

4. RESULTS AND DISCUSSION

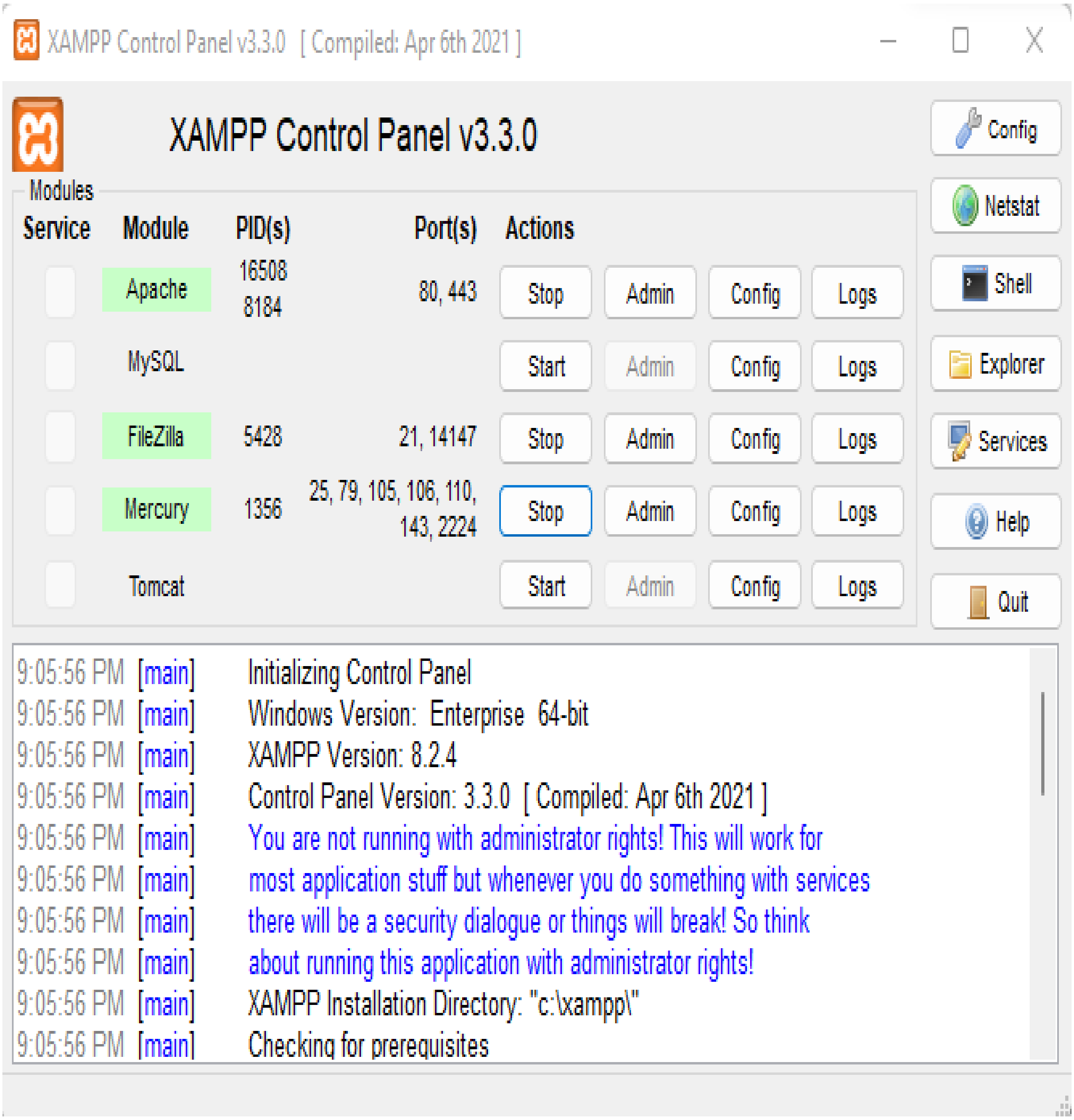
This section displays and discusses the result of the proposed system.

XAMPP interface that should be running for the system to connect to a database. Since the system stores users, logs, detection signatures, or telemetry in MySQL, that database

4.1. Results

The implemented system demonstrated robust performance in secure cloud database access control. Figure 2 shows the

(DB) must be running for the system to function. If Apache or MySQL is stopped, the front end may load but calls to the DB or API will fail and users won't get served.


XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Config
Netstat
Shell
Explorer
Services
Help
Quit

Service	Module	PID(s)	Port(s)	Actions			
	Apache	16508 8184	80, 443	Stop	Admin	Config	Logs
	MySQL			Start	Admin	Config	Logs
	FileZilla	5428	21, 14147	Stop	Admin	Config	Logs
	Mercury	1356	25, 79, 105, 106, 110, 143, 2224	Stop	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
9:05:56 PM  [main]    Initializing Control Panel
9:05:56 PM  [main]    Windows Version:  Enterprise  64-bit
9:05:56 PM  [main]    XAMPP Version: 8.2.4
9:05:56 PM  [main]    Control Panel Version: 3.3.0  [ Compiled: Apr 6th 2021 ]
9:05:56 PM  [main]    You are not running with administrator rights! This will work for
9:05:56 PM  [main]    most application stuff but whenever you do something with services
9:05:56 PM  [main]    there will be a security dialogue or things will break! So think
9:05:56 PM  [main]    about running this application with administrator rights!
9:05:56 PM  [main]    XAMPP Installation Directory: "c:\xampp\"
9:05:56 PM  [main]    Checking for prerequisites
```

Figure 2: XAMPP Control Panel Interface that Illustrates the Backend Database Setup Required for Real-Time Access Verification

Figure 3 shows the login section of the Zero Trust Cloud Database Access Control System. The system employed the concept of least privileged principle which is one of the foundational concepts in cybersecurity and access control. The principle ensures that every user, process, or system component should be granted only the minimum level of access (privileges) necessary to perform its legitimate functions—no more, no less. The system enforces the least privilege principle in multiple layers: User Access Control, Role-Based Access Control (RBAC), Machine Learning Integration, and Zero Trust Verification.

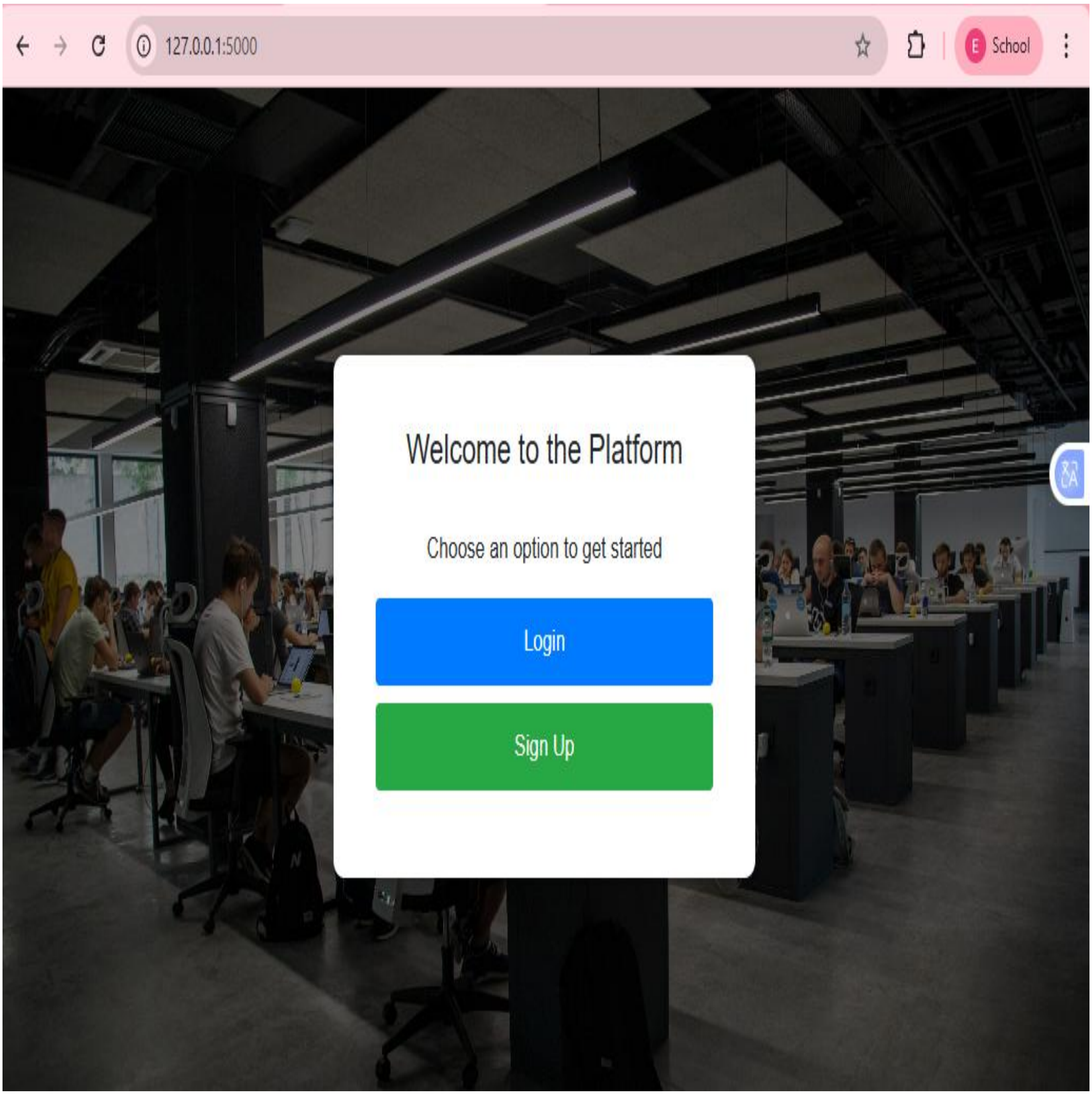
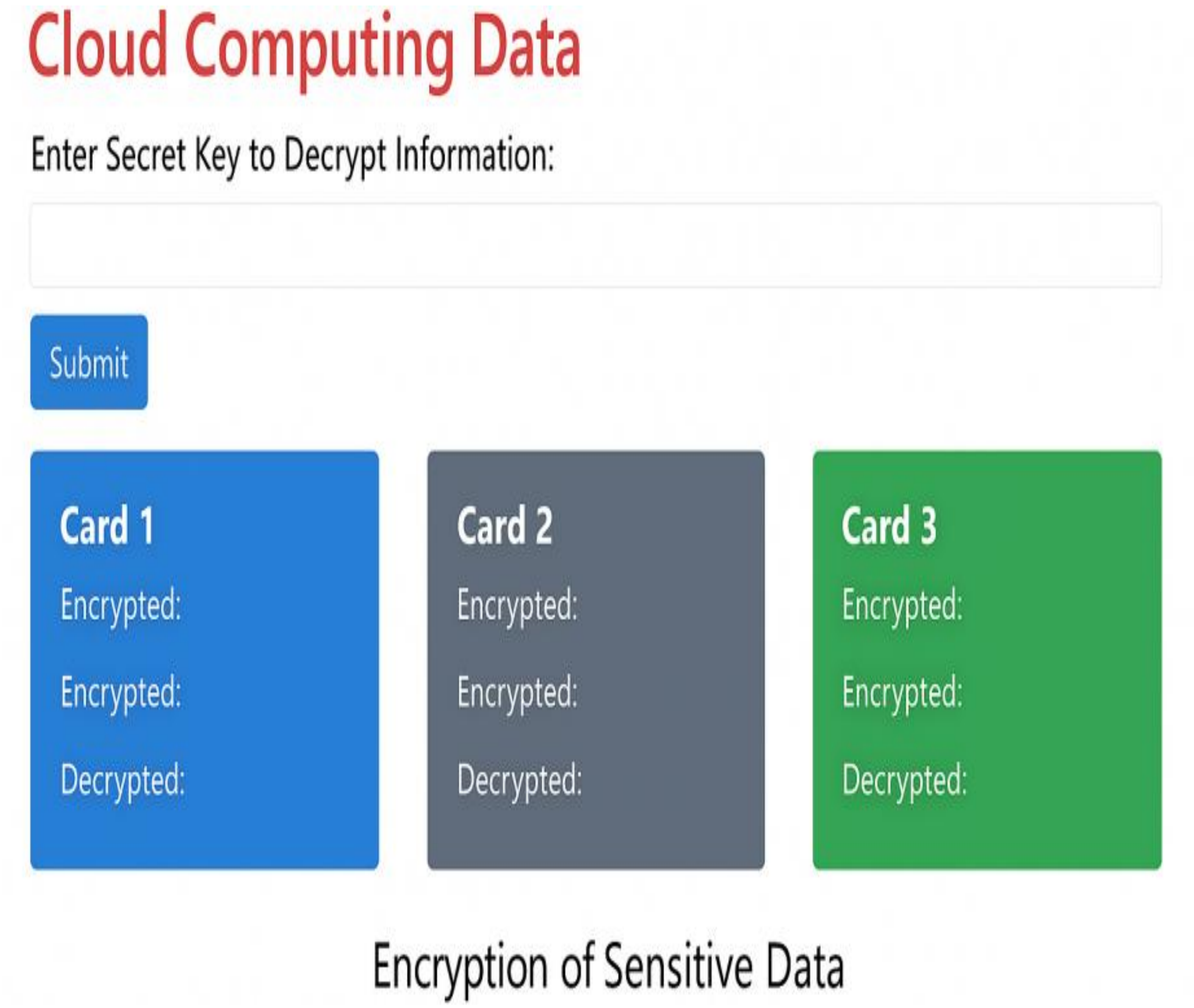


Figure 3: Login Section Implementing the Least Privilege Principle

Figure 4 show encryption and decryption of sensitive data. This figure illustrates how the application implements encryption and decryption of sensitive data within a cloud computing dashboard environment. Each card (Card 1, Card 2, Card 3) contains an "Encrypted" section filled with a long string, which is characteristic of data encoded using cryptographic algorithm. Encryption ensures that even if unauthorized parties gain access to this data, its content remains unreadable without the proper cryptographic key. The dashboard provides a field labeled "Enter Secret Key to Decrypt Information" and a "Submit" button for users to input their decryption key. This enhances the security of sensitive cloud data by enforcing access control and confidentiality. When a secret key is entered, the information on card 1, card 2, and card 3 are decrypted.



Cloud Computing Data

Enter Secret Key to Decrypt Information:

Card 1

Encrypted:

Encrypted:

Decrypted:

Card 2

Encrypted:

Encrypted:

Decrypted:

Card 3

Encrypted:

Encrypted:

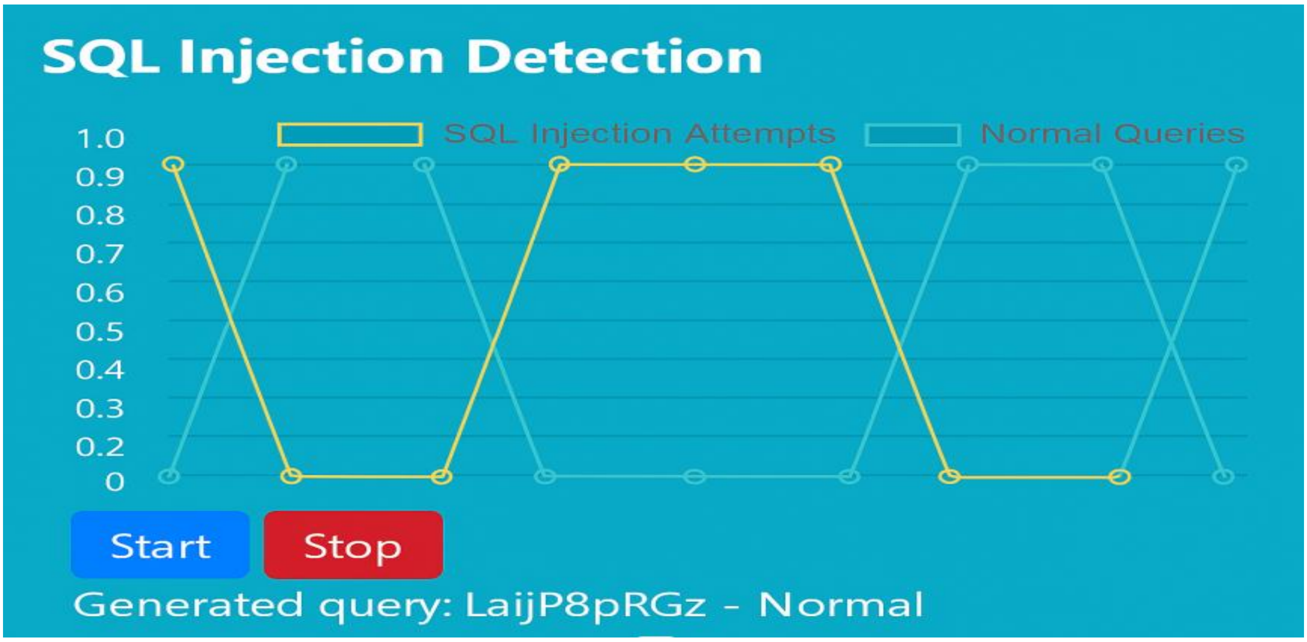
Decrypted:

Encryption of Sensitive Data

Figure 4: Encryption and Decryption Process for Sensitive Cloud Data.

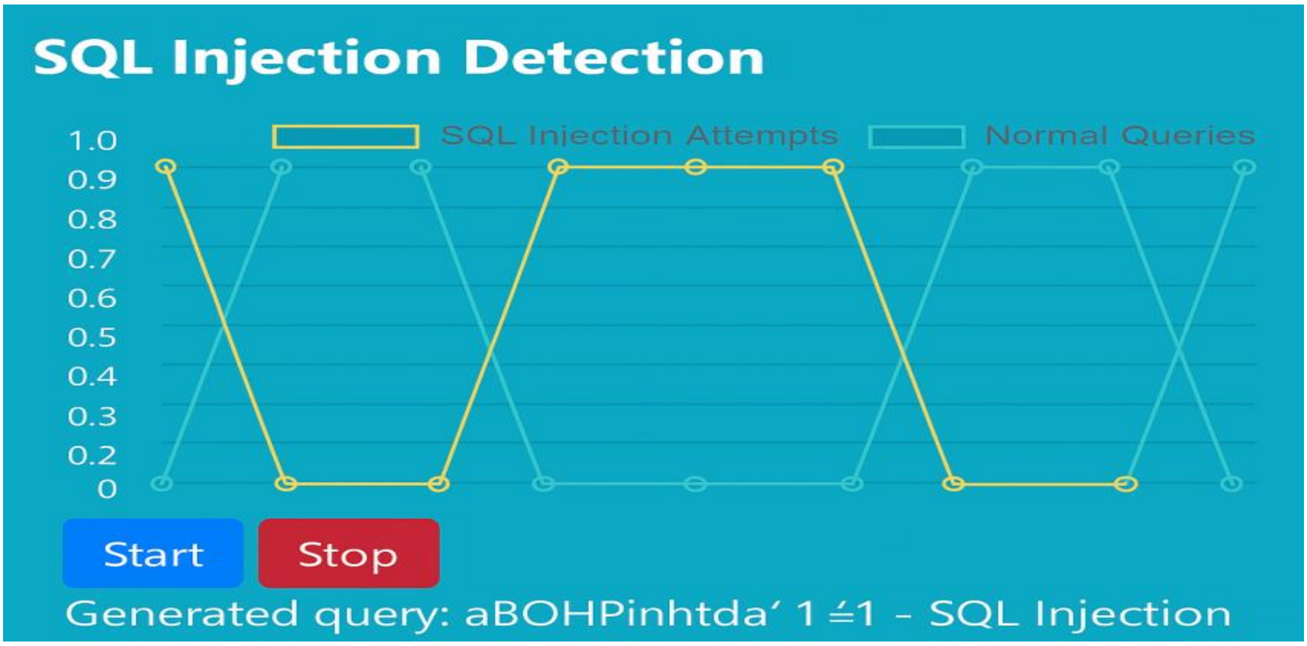
The proposed Zero Trust Cloud Database Access Control system also employs machine learning-driven traffic analysis to distinguish between benign and malicious activities in real-time. This function operates at two critical layers of security:

i. SQL Query Classification (Benign vs. Malign): Detect and prevent SQL injection (SQLi) attacks before they compromise the database. Incoming SQL queries are tokenized, normalized, and passed to a Feed Forward Neural Network (FFNN) model trained on labeled datasets of benign and malicious SQL queries. Feature Extraction includes syntactic elements such as keywords, operators, unusual query length and semantic relationships such as unexpected nesting, concatenations, or tautologies. The model outputs a binary classification: Benign which means query is safe, execution is permitted as shown in Figure 5 and Malign which means query exhibits SQLi patterns, execution is blocked, and alerts are generated as shown in Figure 6. The model achieved 98% classification accuracy. Precision near 100% for benign queries and this minimizes false alarms and 94% precision for malicious queries which ensures most SQL injection attempts are correctly blocked. This proactive classification significantly reduces risks of data leakage, unauthorized modification, or privilege escalation within the database.



Generated query: LaijP8pRGz - Normal

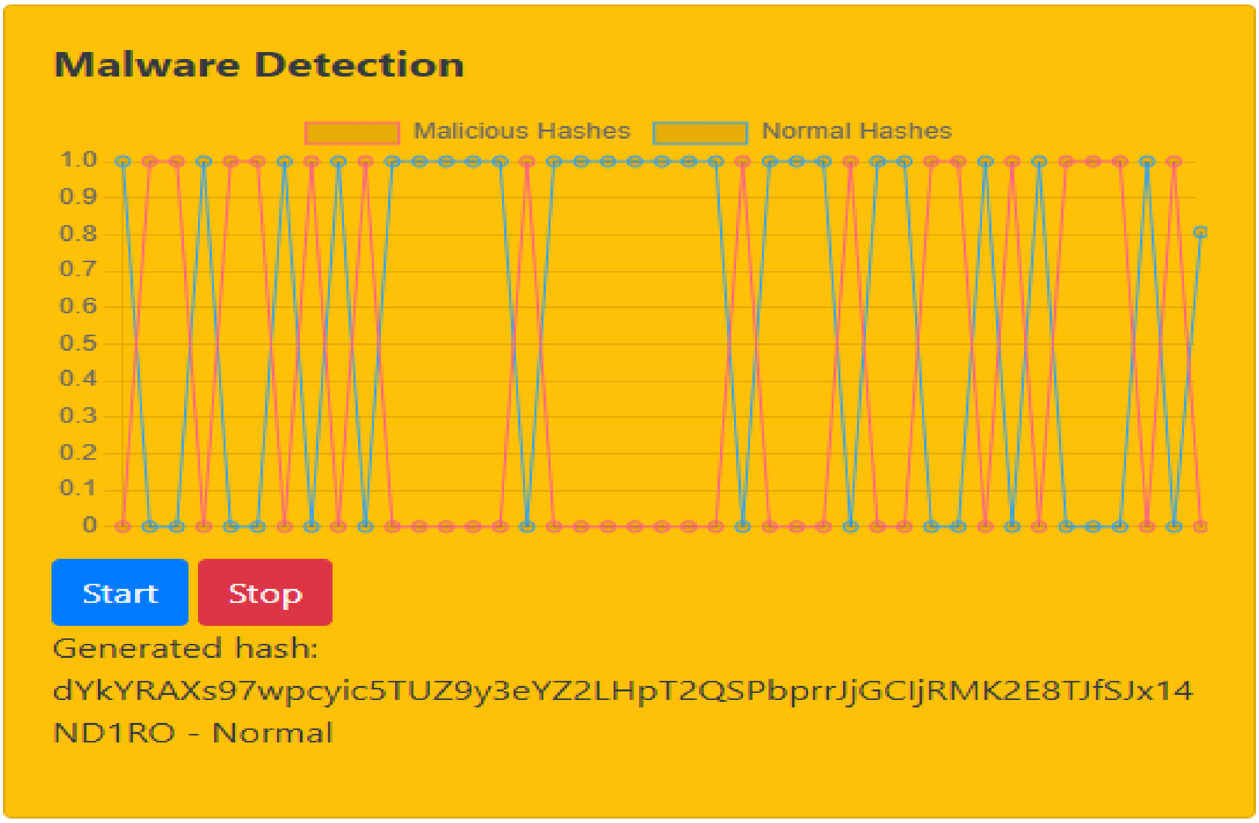
Figure 5: SQL Query Classified as Benign by FFNN Model



Generated query: aBOHPinhtda’ 1 ≐1 - SQL Injection

Figure 6: SQL Query Classified as Malicious by FFNN Model

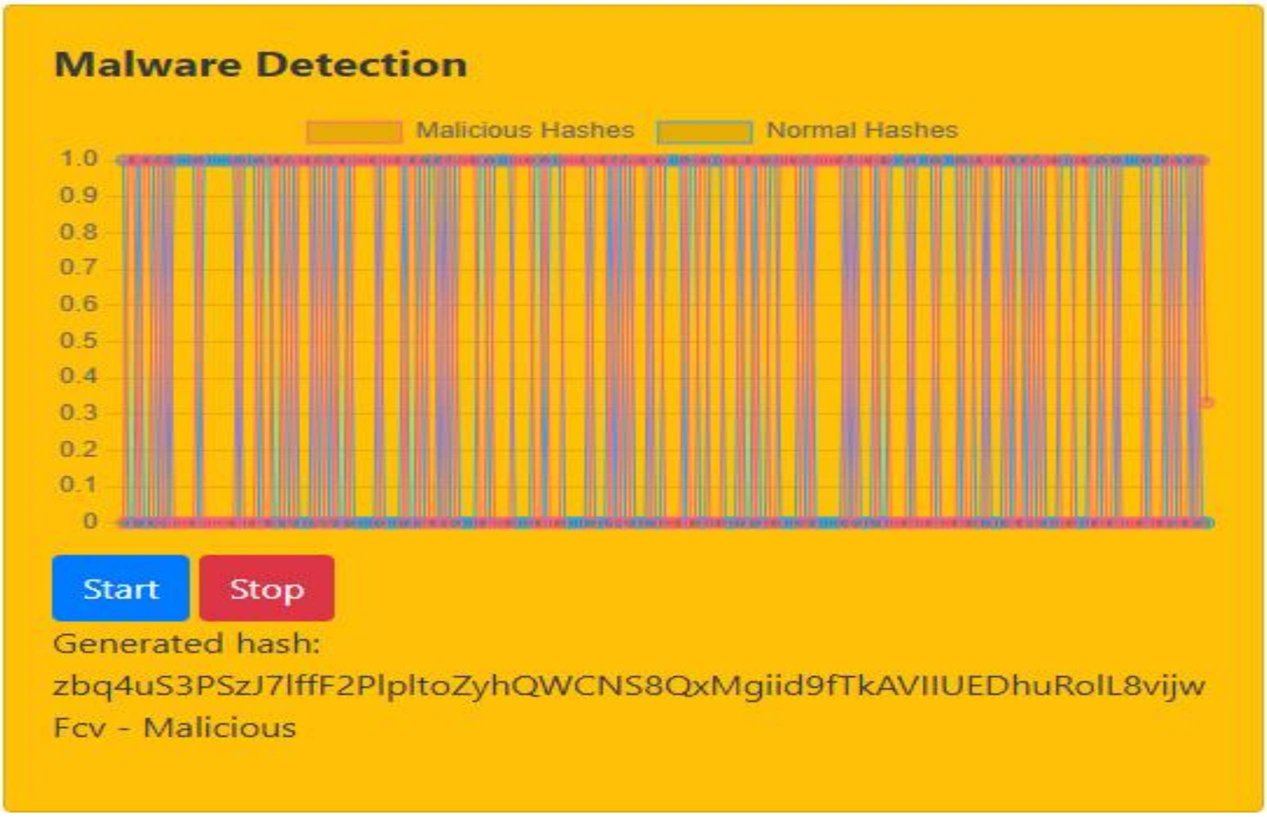
ii. **Malware Traffic Classification (Benign vs. Malign):** Identify malware infiltration attempts through files, network traffic, or suspicious payloads. Behavioral features are extracted from network packets, process behavior, file metadata, and execution patterns. The **Random Forest classifier** is trained to recognize statistical and temporal patterns characteristic of malware. The traffic is classified into benign which means normal traffic, no intervention as shown in figure 7 and Malign which is flagged as malware attempt, blocked, and logged for forensic analysis as shown in figure 8 The Random Forest achieved 99.37% accuracy, underscoring high reliability in detecting malware. This is effective in catching zero-day threats when combined with behavioral analytics, since classification is not limited to known signatures. This layer prevents infiltration of malicious code that could compromise system availability, integrity, or confidentiality.



Malware Detection

Generated hash:
dYkYRAXs97wpcyic5TUZ9y3eYZ2LHpT2QSPbprrJjGCIjRMK2E8TJfSJx14
ND1RO - Normal

Figure 7: Malware Traffic Classified as Benign by Random Forest Model



Malware Detection

Generated hash:
zbq4uS3PSzJ7lffF2PlpltoZyhQWCNS8QxMgiid9fTkAVIIUEDhuRolL8vijw
Fcv - Malicious

Figure 8: Malware Traffic Classified as Malicious by Random Forest Model

4.2. Evaluation Metrics

The performance of the Feedforward Neural Network (FFNN) and Random Forest (RF) classifiers was quantitatively assessed using standard evaluation metrics, including accuracy, precision, recall, and F1-score. These metrics provide a comprehensive understanding of the model's ability to correctly identify SQL injection and malware attacks. Table 1 shows the evaluation metrics of each of the models.

Table1: Evaluation Metrics of FFNN and RF Models

Model	Accuracy (%)	Precision	Recall	F1-Score	Dataset
FFNN	98.00	0.97	0.96	0.965	SQL Injection Dataset
Random Forest	99.37	0.99	0.98	0.985	Malware Dataset

The FFNN model achieved a high detection rate for SQL injection attacks, with minimal false positives. The Random Forest model demonstrated superior generalization, handling diverse malware patterns efficiently.

4.3. Comparative Evaluation

To validate model robustness, the performance of the proposed FFNN and Random Forest classifiers was compared with other conventional models such as Support Vector Machine (SVM) and Logistic Regression. The comparison revealed that deep and ensemble learning methods outperform traditional algorithms under Zero Trust conditions. Table 2 shows the comparative evaluation of FFNN and Random Forest with other models

Table 2: Comparative Evaluation of FFNN and Random Forest with Other Models

Model	Accuracy (%)	Remarks
Logistic Regression	93.00	Struggled with nonlinear feature patterns
Support Vector Machine	95.00	Effective but slower in large-scale classification
FFNN (Proposed)	98.00	Robust feature learning, reduced false positives
Random Forest (Proposed)	99.37	High detection precision and minimal overfitting

This comparative result underscores that combining Zero Trust architecture with machine learning techniques yields improved accuracy and adaptability against evolving security threats.

4.4. Evaluation on Diverse Datasets

The models were further validated using the UNSW-NB15 [31] and ISOT malware datasets[10] to examine their performance in different operational contexts. Both datasets simulate realistic cloud traffic and intrusion patterns. The models maintained accuracy above 97% across datasets, indicating strong generalization capability. These outcomes demonstrate that the integrated system remains effective when subjected to varied and previously unseen data distributions, which is critical for real-world deployment in dynamic cloud environments.

4.5. Discussion of Result

The combination of Zero Trust principles and machine learning techniques has proven effective in mitigating both SQL injection and malware threats. Continuous verification, user behavior profiling, and multi-layered encryption collectively strengthen the security posture of the cloud database. The results indicate that combining zero-trust principles with machine learning and behavioral analytics significantly improves cloud database security. The high detection accuracies of FFNN and Random Forest models confirm the efficacy of leveraging advanced supervised learning techniques for identifying SQL injection and malware attacks. Behavioral analytics add an adaptive layer by continuously monitoring anomalies and adjusting trust scores, facilitating proactive threat mitigation. For the Zero Trust Enforcement, even though a user or process may be authenticated, every query or file hash is re-evaluated at runtime. This reflects the **"never trust, always verify"** principle in practice. Encryption ensures confidentiality without compromising system usability. The system's adaptability and extensibility provide resilience against emerging threats and evolving security requirements, making it a valuable contribution to advancing zero-trust security architectures in cloud database environments. Table 3 provides context and reinforces how our work outperforms prior approaches.

Table 3: Comparative Summary of the Research

Study	Method	Accuracy (%)	Key Limitation
[29] Tripathy et al. (2020)	SVM for SQLI Detection	95.4	Show robustness and reproducibility
[3] Aslan et al. (2021)	Behavior-based Malware Detection	96.2	High false positive rate
Proposed Work	FFNN + RF + Zero Trust	99.37	Needs large-scale validation

5. CONCLUSION

The integration of Zero Trust architecture with intelligent machine learning models and behavioral analytics offers a robust, dynamic, and proactive approach to cloud database security. The research demonstrates that employing supervised learning techniques such as Feedforward Neural Networks and Random Forest classifiers effectively detects SQL injection and malware threats, respectively, achieving high accuracy with minimal false positives. Behavioral analytics provide an adaptive layer that continuously monitors user behaviors, improving the system's ability to identify and respond to insider threats and emerging attack vectors in real-time. The enforcement of Zero Trust principles ensures stringent access controls, minimizing risks associated with unauthorized data access.

Future scope should incorporate federated learning to enable privacy-preserving training across distributed cloud systems, explore reinforcement learning for adaptive, real-time policy adjustments, and apply Explainable AI (XAI) to improve interpretability of threat detection results.

6. ACKNOWLEDGMENT

Our thanks to the Almighty God for His grace and Strength.

7. REFERENCES

[1] Aboh, U., Moustafa, N., & Janjua, Z. H. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11,* 91. Springer.

[2] Aryal, K., Gupta, M., & Abdelsalam, M. (2022). Analysis of label-flip poisoning attack on machine learning based malware detector. *2022 IEEE International Conference on Big Data (Big Data)* (pp. 4236–4245). IEEE.

[3] Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). Intelligent behavior-based malware detection system on cloud computing environment. *IEEE Access, 9,* 83252–83271.

[4] Gandhi, N., Mishra, S., Patel, J., Doshi, N., & Sisodiya, R. (2021). A CNN-BiLSTM based approach for detection of SQL injection attacks. *2021 6th International Conference for Convergence in Technology (I2CT)* (pp. 378–383). IEEE.

[5] Gyamfi, N. K., Goranin, N., Čenys, H. A., & Ceponis, D. (2023). Automated system-level malware detection using machine learning: A comprehensive review. *Applied Sciences, 13*(21), 11908. MDPI.

[6] Hasan, M., Tarique, M., & Balbahaith, Z. (2019). Detection of SQL injection attacks: A machine learning approach. *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)* (pp. 1–6). IEEE.

[7] He, P., Ji, S., Xia, Y., & Zhang, X. (2023). Efficient query-based attack against ML-based Android malware detection under zero knowledge setting. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 90–104). ACM.

[8] Hidayat, T., & Mahardiko, R. (2020). A systematic literature review method on AES algorithm for data sharing encryption on cloud computing. *International Journal of Artificial Intelligence Research, 4*(1).

[9] Ige, T., & Sikiru, A. (2022). Implementation of data mining on a secure cloud computing over a web API using supervised machine learning algorithm. In R. Silhavy (Ed.), *Artificial Intelligence Trends in Systems. CSOC 2022. Lecture Notes in Networks and Systems* (Vol. 502, pp. 203–210). Springer, Cham.

[10] ISOT Malware Dataset. (2023). University of Victoria, Canada. Available at: https://www.uvic.ca/engineering/isot/datasets/

[11] Khan, N., & Al-Yasiri, A. (2016). Cloud security threats and techniques to strengthen cloud computing adoption framework. *International Journal of Information Technology and Web Engineering, 11*(3), 50–64. IGI Global.

[12] Kurniawan, H., Rosmansyah, Y., & Dabarsyah, B. (2015, August). Android anomaly detection system using machine learning classification. In *Proceedings of the 2015 International Conference on Electrical Engineering and Informatics (ICEEI)* (pp. 288–293). IEEE.

[13] Markel, Z., & Bilzor, M. (2014, October). Building a machine learning classifier for malware detection. In *Proceedings of the 2014 Second Workshop on Anti-Malware Testing Research (WATeR)* (pp. 1–4). IEEE.

[14] Mohamad, N. H., Zaidi, M. I. H. B., & Saidin, N. B. (2023). Data security and privacy issues in cloud computing: Challenges and solutions review. *Institute of Electrical and Electronics Engineers (IEEE).*

[15] MongoDB. (2024). Cloud database overview. Retrieved September 22, 2025, from https://www.mongodb.com.

[16] Nikos, A., Basu, S., Bhanoori, N., et al. (2022). Amazon Redshift. Re-invented. In *Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD '22)* (pp. 2205–2217). ACM.

[17] Nnodi, J. T., & Obasi, E. C. M. (2025). Leveraging artificial intelligence for detecting insider threats in corporate networks. *University of Ibadan Journal of Science and Logics in ICT Research, 13*(1), 130–144.

[18] Obasi, E. C. M., & Abosede, O. (2025). Leveraging machine learning algorithms for enhanced prediction of product yields and purity in chemical reactions. *Nile Journal of Engineering and Applied Sciences.*

[19] Obasi, E. C. M., & Nlerum, P. A. (2023). A model for the detection and prevention of backdoor attacks using CNN with federated learning. *University of Ibadan Journal of Science and Logics in ICT Research, 10*(1), 9–21.

[20] Obasi, E. C. M., & Stow, M. T. (2023). A predictive model for uncertainty analysis on big data using Bayesian CNN. *University of Ibadan Journal of Science and Logics in ICT Research, 9*(1), 52–62.

[21] Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of Cyber Security,* 115–133.

[22] Panker, T., & Nissim, N. (2021). Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux cloud environments. *Knowledge-Based Systems, 226,* 107095. Elsevier.

[23] Shariati, S. M., Ahmadzadegan, M. H., & Abouzarjomehri, A. (2015). Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection. *2015 International Conference on Computer, Communication and Control (IC4)* (pp. 1078–1082). IEEE.

[24] Singhal, S., Srivastava, R., Shyam, R., & Mangal, D. (2023). Supervised machine learning for cloud security. *2023 6th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1–5). IEEE.

[25] Stow, M. T., & Obasi, E. C. M. (2025). An interpretable early warning system for malaria outbreak in Bayelsa State using deep learning and climate data. *International Journal of Advanced Research in Computer and Communication Engineering, 14*(8), 58–101.

[26] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing, 76*(12), 9493–9532. Springer.

[27] Tianfield, H. (2012). Security issues in cloud computing. *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 1082–1089). IEEE.

[28] Timadi, M. E., & Obasi, E. C. M. (2025). Integrating zero-trust architecture with deep learning algorithm to prevent structured query language injection attack in cloud database. *University of Ibadan Journal of Science and Logics in ICT Research, 13*(1), 52–62.

[29] Tripathy, D., Gohil, R., & Halabi, T. (2020, May). Detecting SQL injection attacks in cloud SaaS using machine learning. In *Proceedings of the 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data & Security (IDS)* (pp. 145–150). IEEE.

[30] Uwagbole, S. O., Fan, L., & Buchanan, W. J. (2017). Applied machine learning predictive analytics to SQL injection attack detection and prevention. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 1087–1090). IEEE.

[31] UNSW-NB15 Dataset. (2023). University of New South Wales. Available at: https://research.unsw.edu.au/projects/unsw-nb15-dataset.

[32] Xu, Z., Ray, S., Subramanyan, P., & Malik, S. (2017). Malware detection using machine learning-based analysis of virtual memory access patterns. In *Proceedings of the 2017 Design, Automation and Test in Europe (DATE 2017)* (pp. 169–174). IEEE.