Journal of
Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.070952

ARTICLE

An Intelligent Zero Trust Architecture Model for Mitigating Authentication Threats and Vulnerabilities in Cloud-Based Services

Victor Otieno Mony*, Anselemo Peters Ikoha and Roselida O. Maroko

Department of Information Technology, School of Computing & Informatics, Kibabii University, Bungoma, 50200, Kenya

*Corresponding Author: Victor Otieno Mony. Email: victor@rcadventist.org

Received: 28 July 2025; Accepted: 27 August 2025; Published: 30 September 2025

ABSTRACT: The widespread adoption of Cloud-Based Services has significantly increased the surface area for cyber threats, particularly targeting authentication mechanisms, which remain among the most vulnerable components of cloud security. This study aimed to address these challenges by developing and evaluating an Intelligent Zero Trust Architecture model tailored to mitigate authentication-related threats in Cloud-Based Services environments. Data was sourced from public repositories, including Kaggle and the National Institute for Standards and Technology MITRE Corporation's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) framework. The study utilized two trust signals: Behavioral targeting system users and Contextual targeting system devices. Based on the trust signals, two machine learning models—Keystroke Dynamics and Device Location—were developed using Binary Logistic Regression, achieving a combined average accuracy of 80.63%, with a residual ineffectiveness rate of 19.37%. The Intelligent Zero-Trust Architecture Threat Mitigation Model was introduced to reclassify threat severity scores, resulting in the downgrading of all authentication threats to Low Severity, demonstrating a mitigation effectiveness exceeding 80%. This research contributes to the field of cybersecurity by presenting a validated, intelligent, and context-aware Intelligent Zero-Trust Architecture model capable of enhancing identity and access management in dynamic cloud environments. The findings offer actionable insights for cloud architects, cybersecurity professionals, and policymakers aiming to strengthen trust, reduce attack surfaces, and improve threat resilience across digital infrastructure.

KEYWORDS: Cloud-based services; zero trust architecture; intelligent zero trust architecture; cloud computing; cloud authentication; machine learning; binary logistics regression; loss function; holdout validation; confusion matrix; precision rates; negative predictive value

1 Introduction

Zero Trust Architecture (ZTA) has emerged as a transformative framework in modern cybersecurity, particularly for cloud-based environments where traditional perimeter-based security models are insufficient. Rooted in the principle of "never trust, always verify," ZTA mandates continuous validation of users, devices, and network behavior before granting access to resources [1]. ZTA is a promising paradigm to counter Cloud-based Services (CBS) authentication challenges because it enforces strict access controls, continuous verification, and the principles of least privilege, while providing enhanced visibility and analytics for improved decision-making across cloud environments [2]. Unlike perimeter-based models, ZTA treats every access request as untrusted by default, thus offering a more granular and dynamic approach to cloud security. Zero-trust is growing in favor in cloud environments as a means through which unauthorized access can be mitigated. Thus, it enables a more successful prevention mechanism against advanced assaults [3].

This paradigm shift addresses the increasing sophistication of cyber threats and the vulnerabilities arising from distributed systems, remote work, and hybrid cloud architectures.

Cloud systems are particularly vulnerable due to their shared and complex systems [3]. CBS enables users to interact directly with cloud-based applications, making it especially vulnerable to attacks that exploit weak authentication mechanisms [4,5]. Researchers have proposed emerging solutions, including decentralized identity protocols, blockchain-based authentication, and lightweight key exchange protocols [6,7]. Nonetheless, many of these innovations face practical limitations when implemented in the dynamic, distributed cloud environments. For example, while blockchain offers immutability, it does not address the problem of real-time verification of user behavior.

The Kerberos protocol used in distributed authentication systems relies on the Key Distribution Center (KDC) and the Key Distribution System (KDS), which utilize public keys to strengthen data confidentiality and secure messages. Authentication in the protocol Kerberos is done through a unique ticket system. The tickets are granted through a KDC hosted on third-party servers to provide scalability [8,9].

The Kerberos protocol relies on symmetric key encryption but is vulnerable to dictionary and brute-force attacks if weak passwords are used [8]. Symmetric keys used in Kerberos also lead to the likelihood of data breaches when the KDC is compromised. Further, Kerberos provides the public key at both ends of data transit, and this is a vulnerability that can be exploited using means such as Denial of Service Attacks. Kerberos also relies on trusted third-party servers, which may lead to insider attacks and cause serious data breaches. A dictionary attack on the Kerberos protocol can steal passwords by interrupting data flow. A compromise in the tickets by threat actors leads to a compromise in the KDC. This is because Kerberos utilizes symmetric encryption, where a single unique key is utilized, and this increases its vulnerability should the key be compromised. Further, in symmetric key cryptography, the algorithms used, such as Advanced Encryption Standard (AES), are increasingly becoming vulnerable in the face of quantum computing threats [8,9].

Likewise, public key infrastructure (PKI)-based authentication often requires physical tokens or one-time password generators, posing usability and manageability challenges [10]. These vulnerabilities highlight the inadequacy of traditional perimeter-based security models, which often assume implicit trust once access is granted. In response to these threats and vulnerabilities, there has been a shift toward stronger authentication mechanisms, such as two-factor authentication (2FA), multi-factor authentication (MFA), and behavioral biometrics [11]. The emergence of quantum computing further exacerbates the situation by threatening to render many of today's encryption algorithms obsolete [3]. The crypto market disruptions of 2022 underscored the urgency of rethinking foundational security mechanisms [12]. Insider threats and third-party risks compound the problem, as trusted users may become inadvertent attack vectors by leaking credentials or bypassing controls [13]. Against this backdrop, Zero Trust Architecture (ZTA) has gained prominence as a paradigm shift in cybersecurity.

Research literature reveals a decisive transition from traditional perimeter-based security models to identity-centric frameworks such as Zero Trust Architecture (ZTA). This shift is motivated by the inadequacy of conventional security measures to address modern cyber threats in cloud-based services. ZTA emphasizes continuous verification of both user identity and device posture, rejecting the notion of implicit trust within internal networks. As a result, organizations are adopting ZTA to minimize attack surfaces and enforce context-aware access control [14,15].

Another notable trend is the integration of Artificial Intelligence (AI) and Machine Learning (ML) into ZTA frameworks. Intelligent security models that utilize behavioral analytics and real-time threat detection are being developed to enhance the adaptability and precision of access decisions [16]. These

systems dynamically calculate trust scores based on various contextual inputs, including user behavior anomalies, device health, and location data. Furthermore, behavioral biometrics such as keystroke dynamics are increasingly being explored to improve the reliability of user authentication [17].

Multi-cloud and federated environments are also influencing the evolution of ZTA implementations. With cloud services becoming more distributed, organizations face new challenges in enforcing consistent security policies across heterogeneous platforms. Consequently, researchers are focusing on federated learning, decentralized policy engines, and cross-domain trust models to ensure robust authentication across complex cloud ecosystems [18].

Despite these advancements, several gaps persist in the literature. First, there is a lack of empirical validation for most Intelligent Zero Trust Architecture (IZTA) models. Many proposed frameworks remain conceptual or are only tested through limited simulations, failing to demonstrate their effectiveness in real-world SaaS or hybrid cloud environments [19]. This gap limits the generalizability and practical application of existing models.

Secondly, the underutilization of multi-modal trust signals is a recurring limitation. Most ZTA models rely on a narrow range of indicators—such as static credentials, IP reputation, or device fingerprints—without integrating more diverse behavioral and environmental data. The failure to incorporate factors like keystroke dynamics, geo-location, user intent, and biometric feedback reduces the models' responsiveness to nuanced threat vectors [20].

Another critical gap involves the explainability of AI-driven access decisions. Many ML-based ZTA models operate as "black boxes," making it difficult for system administrators to understand why access is granted or denied. This lack of transparency raises compliance concerns and impairs user trust in the system [3,21]. In addition, performance challenges such as computational latency and resource overhead further complicate real-time deployment of intelligent authentication mechanisms in high-volume environments [16]. Table 1 gives a summary of the identified research gaps in the literature:

Table 1: Identified knowledge gaps and the study's strategic response

Theme	Author(s)	Key findings	Identified gap	How the study filled the gap
Lack of empirical validation	Wei (2023) [19]	Most Intelligent Zero Trust Architecture (IZTA) frameworks are theoretical, with limited real-world testing in CBS environments.	Inadequate empirical validation of IZTA models limits their credibility and scalability in actual SaaS, IaaS, or hybrid cloud environments.	The present study simulated authentication scenarios in a CBS environment, implemented an IZTA model, and evaluated it using real-world threat vectors and supervised ML performance metrics.
Underutilization of multi-modal trust signals	Tiwari et al. (2021) [20]; Kancherla. (2025) [16]	Traditional ZTA implementations rely heavily on static or narrow trust indicators such as passwords or IP addresses.	Absence of integrated behavioral and contextual data (e.g., keystroke dynamics, geo-location, session metadata) undermines dynamic threat recognition.	The IZTA model combines keystroke biometrics with contextual trust signals, enabling dynamic authentication based on real-time user behavior and device context.

(Continued)

Table 1 (continued)

Theme	Author(s)	Key findings	Identified gap	How the study filled the gap
Explainability of AI models	Zhou et al. (2023) [17]	Most ML-based Zero Trust systems are opaque, offering no clarity on access decisions.	Limited explainability of ML models hinders trust, auditability, and compliance with data governance regulations in cloud environments.	The study used interpretable ML techniques (binary logistic regression) that generate transparent trust scores and allow administrators to trace decisions for each authentication request.
Performance limitations	Wang et al. (2023) [18]	Many intelligent ZTA models introduce latency and require significant computational resources, which makes real-time deployment impractical.	High latency and resource constraints restrict the real-time applicability of ML-driven access controls in cloud services.	The IZTA framework was optimized using feature engineering and lightweight ML models to enable efficient decision-making without compromising security in real-time cloud environment.

ZTA assumes no trust by default, requiring continuous verification of user identity, device health, location context, and access behaviors [1] and enforces principles such as least privilege access, micro-segmentation, and context-aware authorization, significantly reducing the attack surface [3]. However, the application of intelligent provisioning within ZTA frameworks, especially in cloud-based authentication, remains limited in research and practice. This study addresses this gap by proposing the Intelligent Zero Trust Architecture (IZTA) model; a framework that integrates machine learning algorithms and behavioral analytics into ZTA for dynamic authentication. The research explores how keystroke dynamics, device location, and other contextual trust signals can be used to enhance real-time access control decisions. By designing and evaluating an IZTA model specifically for Cloud-Based Services (CBS), the study contributes a novel, data-driven solution to the persistent security threats in cloud authentication systems.

2 Methods

This study employs a quasi-experimental research design to develop and evaluate an Intelligent Zero Trust Architecture (IZTA) model capable of mitigating authentication threats in Cloud-Based Services (CBS). A quasi-experimental approach is selected due to the practical limitations associated with random assignment and control of real-world cloud security environments. Unlike purely experimental designs, quasi-experiments allowed for comparative evaluation across controlled and treatment scenarios using existing datasets and systems. The evaluation of Zero Trust Architecture (ZTA) principles relevant to mitigating CBS threats and vulnerabilities was performed, and a ZTA-based integration model was formulated and tested under varying threat conditions to determine its effectiveness. The final phase involved the design, training, and implementation of the IZTA model using supervised machine learning techniques, particularly binary logistic regression.

To simulate the experimental process, two comparison scenarios were established:

i. **Control Scenario**—where authentication threats were analyzed under existing, non-ZTA-based security frameworks.

ii. **Treatment Scenario**—where the same threats were analyzed under dynamic ZTA configurations based on contextual and behavioral trust indicators.

Given the nature of the research, which focuses on behavioral authentication, contextual access, and threat mitigation in cloud environments, the data collection strategy is designed to obtain large, high-quality datasets containing relevant variables such as keystroke dynamics, device telemetry, geolocation access records, and known attack vectors. The data is sourced from reputable public repositories and cybersecurity research platforms, including Kaggle Data Warehouse, National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD), the MITRE ATT&CK Framework, and curated datasets available through academic and industry research portals. The data collection process employed a hybrid toolset comprising Extract, Load, and Transform (ELT) pipelines, Python-based data preparation frameworks, web scraping utilities, and standardized threat databases. This comprehensive toolset ensured that the data used in the study was not only extensive and diverse but also aligned with the latest cybersecurity standards and real-world threat scenarios. The accuracy of the resulting datasets was crucial in training the machine learning models and validating the robustness of the proposed IZTA model.

To establish and maintain high-quality standards, this study employed a multi-pronged quality control strategy spanning data preparation, model development, evaluation, and ethical safeguards. For validity, the study employed holdout validation to ascertain predictive validity by dividing the training and test datasets into a 70:30 percentage ratio. To ascertain Machine Learning (ML) models' validity, the cross-entropy loss function formula was applied, and to ascertain the IZTA model's validity, five experts in the field of Information Technology and cybersecurity were employed. Reliability is the quality of trustworthiness of the results of a study. This study ascertained ML models' reliability through the extraction of a confusion matrix, which helped in the calculations of the Negative Predictive Value (NPV) and the Precision Rates (PR). Process reliability was attained through Python libraries, and Binary Logistic Regression algorithms.

The study employed a supervised machine learning algorithm, binary logistic regression under binary classification, which was selected for its transparency, interpretability, and proven performance in security prediction tasks. Binary Logistic Regression is chosen for its interpretability compared to non-linear or high-dimensional models such as neural networks, which are far more complex and require more overhead costs to implement. Further, Binary logistic regression is the most suitable algorithm for this study due to its interpretability, efficiency, and robustness in binary classification problems. Since the authentication outcome is inherently binary, grant or deny access, the model aligns naturally with logistic regression's predictive objective of estimating probabilities between two discrete classes. Unlike more complex black-box models (e.g., deep neural networks), logistic regression offers clear insight into how each input feature (e.g., typing rhythm, device location, session time) contributes to the final decision, which is critical for building explainable and auditable trust systems. Furthermore, logistic regression performs well with moderately sized and clean datasets, requires relatively low computational resources, and can handle collinear features through regularization techniques, making it ideal for cloud authentication use cases where real-time processing and clarity of outcomes are paramount. This balance of accuracy, transparency, and computational feasibility makes Binary Logistic Regression the preferred algorithm for developing and evaluating the proposed Intelligent Zero Trust Architecture (IZTA) model.

Two IZTA model prototypes were developed using different combinations of features (e.g., keystroke dynamics, location data, session attributes), and their outputs were compared for consistency in results. The confusion matrix was used as a key tool to analyze true positives, false positives, true negatives, and false negatives, thereby providing an empirical measure of the model's reliability across test cases. Furthermore, quality control extended to data preprocessing, where Python libraries such as Pandas were used for dataset cleansing and normalization to eliminate noise, redundancies, and inconsistencies that could bias

the machine learning outcomes. Data visualization tools, including Matplotlib, were utilized to inspect and confirm the presence of logical patterns and trends before model training commenced. The emphasis on both technical accuracy and conceptual integrity ensured that the IZTA model developed through this study is both scientifically valid and practically deployable in real-world cloud security contexts.

All datasets were anonymized, de-identified, and processed in line with data protection guidelines. No attempt was made to reverse-engineer personal identities, and all analytic procedures focused solely on behavioral patterns, device metadata, and security event logs in abstracted formats. Furthermore, all digital tools, software libraries (e.g., Pandas, Matplotlib), and databases (e.g., Kaggle, NIST Threat Mitre Framework) were used under their respective open-source or academic research licenses. This study upheld ethical rigor across all phases from conceptualization and data acquisition to analysis and reporting, ensuring that its outputs are ethically sound, legally compliant, and academically trustworthy.

The initial phase of IZTA model development involves identifying and acquiring datasets that provide reliable indicators for behavioral and contextual authentication. Specifically, this study focuses on datasets related to keystroke dynamics and device location two critical attributes in determining user and device trust levels within a Zero Trust Architecture framework. Both datasets were sourced from the publicly accessible Kaggle data repository. Table 2 provides a metadata summary of the selected datasets.

Table 2: Datasets for IZTA model development (accessed on 26 August 2025)

No.	Dataset name	Dataset location	Dataset size
1.	Location Intelligence Cybersecurity 2025	https://www.kaggle.com/datasets/wisam1985/location-intelligence-for-cybersecurity-2025	65,450 Records
2.	DSL-StrongPasswordData	https://www.kaggle.com/datasets/carnegiecylab/keystroke-dynamics-benchmark-data-set	20,400 Records

The training algorithm begins by loading the preprocessed device location dataset, followed by the separation of features (latitude and longitude) and labels (trust classifications). These features are then normalized and divided into training and test sets, maintaining a 70:30 ratio as previously established. The fit function of the binary logistic regression model is invoked to initiate the training process, during which the model iteratively learns optimal weights for the features using gradient descent and minimizes the loss function. The model learns to differentiate trusted from untrusted login attempts based on proximity to known threat hotspots. After training, the predict function is employed to evaluate the model's performance on the test dataset, with results further validated using accuracy, precision, recall, and the confusion matrix. By training the model on location-based contextual features, the IZTA framework is empowered to make informed trust decisions grounded in both spatial intelligence and behavioral insights. This enhances its alignment with Zero Trust principles, where every access request must be continuously verified before being granted.

Ethical Considerations and Data Privacy

Ethical compliance is a fundamental pillar of any credible research study, and this study adhered to established ethical standards throughout its lifecycle. The study primarily utilized non-human, secondary data sources such as publicly available datasets on keystroke dynamics, device locations, authentication events, and threat intelligence, which minimized the risk of ethical breaches involving human participants.

Although the data used did not involve direct human subjects, stringent measures were implemented to ensure the privacy, confidentiality, and integrity of the information analyzed. All datasets were anonymized,

de-identified, and processed in line with data protection guidelines. No attempt was made to reverse-engineer personal identities, and all analytic procedures focused solely on behavioral patterns, device metadata, and security event logs in abstracted formats.

Furthermore, all digital tools, software libraries (e.g., Pandas, Matplotlib), and databases (e.g., Kaggle, NIST Threat Mitre Framework) were used under their respective open-source or academic research licenses. Proper attribution and citation of external works and data sources were maintained throughout the documentation and writing of this thesis.

In keeping with academic integrity, the contributions of other authors, datasets, and prior research were fully acknowledged. No part of the work involved plagiarism or data falsification, and care was taken to preserve transparency in the research design, implementation, and reporting process. This study upheld ethical rigor across all phases from conceptualization and data acquisition to analysis and reporting, ensuring that its outputs are ethically sound, legally compliant, and academically trustworthy.

3 Results

To evaluate the performance of the Intelligent Zero Trust Architecture (IZTA) models, the study employed two machine learning classifiers developed using binary logistic regression: one trained on the **Keystroke Dynamics** dataset and the other on the **Device Location** dataset. Both models were designed to classify authentication attempts as legitimate or malicious, based on behavioral and contextual trust indicators, respectively.

As shown in Fig. 1, training algorithms incorporate **cross-entropy loss functions** as part of their learning processes. These functions serve as core validity indicators, enabling the models to minimize error through iterative optimization and to compute reliable weight and bias parameters that improve predictive accuracy.

```
import pandas as pd
import numpy as np
from sklearn.model_selection import train_test_split
from LogisticRegression import LogisticRegression

bc = pd.read_csv(r"C:\Users\victo\Documents\Dataset\LocationDataset.csv")

X = bc.drop (columns = ['ID', 'Cyber Attack Type', 'IoT Device Type','IoT Device Category', 'classifier'], axis = 1)
Y = bc['classifier']

y = Y.values
X = X.values

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.30, random_state=1234)

clf = LogisticRegression()
clf.fit(X_train, y_train)
y_pred = clf.predict(X_test)


def accuracy(y_pred, y_test):
    return np.sum(y_pred == y_test) / len(y_test)
```

Figure 1: Training algorithms for device location

Model validity is assessed through the accuracy score—the proportion of correct predictions out of total predictions—while reliability is evaluated using a confusion matrix, which measures true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN).

3.1 Keystroke Dynamics Model Evaluation

The binary logistic regression model trained on the keystroke dynamics dataset demonstrated an accuracy score of 0.8766, as shown in Fig. 2.

Figure 2: Keystroke dynamics model performance evaluation (loss function)

The high accuracy in the loss function, as depicted by Fig. 2, underscores the model's effectiveness in distinguishing between legitimate and suspicious typing behaviors. As a behavioral trust metric, keystroke dynamics proved to be a robust input for the IZTA authentication logic.

The confusion matrix for keystroke dynamics presented in Fig. 3 confirms this result:

A. True Negatives: 5367 malicious login attempts were correctly identified.
B. False Negatives: 753 login attempts were incorrectly classified.

To validate Keystroke dynamics reliability and its role in the overall trust evaluation process within IZTA, the keystroke dynamics confusion matrix is used by the study to measure the Negative Predictive Value (NPV), which is the determinant of how reliable a negative prediction is. The formula for NPV is:

$$\text{NPV} = \frac{\text{True Negative}}{\text{True Negative} + \text{False Negative}}$$

therefore

$$\text{NPV} = \frac{5367}{5367} + 753$$

$$\textbf{NPV = 0.876956} \quad (1)$$

Eq. (1): Negative Predictive Value for Keystroke Dynamics

Eq. (1) indicates the ability of the keystroke dynamics algorithms to reliably predict a threat actor's keystroke dynamics at 87.696% during the authentication process.

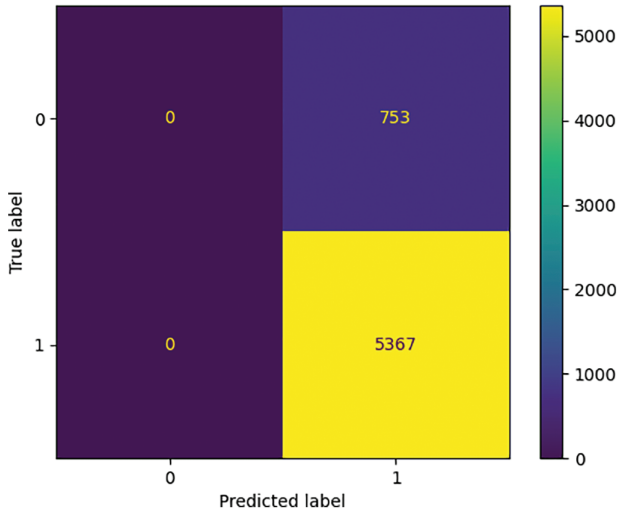

Figure 3: The confusion matrix for keystroke dynamics

3.2 Device Location Model Evaluation

The second binary logistic regression model, developed using device location data, yielded an accuracy score of 0.7357, as depicted in Fig. 4.

```
def accuracy(y_pred, y_test):
    return np.sum(y_pred == y_test) / len(y_test)


acc = accuracy(y_pred, y_test)
print(acc)

✓ [9] 496ms
0.7357270180799592
```

Figure 4: Device location model performance evaluation (loss function)

Although Fig. 4 depicts accuracy scores that are lower than those of the keystroke dynamics model, this result still demonstrates strong predictive ability, particularly in identifying threat actors based on proximity to known attack hotspots. The model leveraged geospatial intelligence to assess risk context, enhancing the granularity of trust decisions. Cross-entropy loss and convergence through gradient descent were similarly applied, and reliability was also validated using a confusion matrix (see Fig. 5).

The confusion matrix for Device Location presented in Fig. 5 confirms this result:

A. True Positives: 14,446 Device Login Locations with CBS Authentication threats were correctly identified.
B. False Positives: 5189 Device Login Locations were incorrectly classified as having CBS authentication threats.

To validate the Device Location Algorithm's reliability and its role in the overall trust evaluation process within IZTA, the device location confusion matrix presented in Fig. 5 is used by the study to measure the Precision Rate (PR), which is the determinant of how reliable a positive prediction is. Eq. (2) presents the equation for PR.

$$PR = \frac{TruePositive}{TruePositive + FalsePositive}$$

$$therefore$$

$$PR = \frac{14{,}496}{14{,}496 + 5189}$$

$$PR = 0.7357 \quad (2)$$

Eq. (2): Precision Rates for Device Location

Eq. (2) indicates the ability of the Device Location algorithm to reliably predict the proximity of devices to locations with CBS authentication threats by 73.57%.

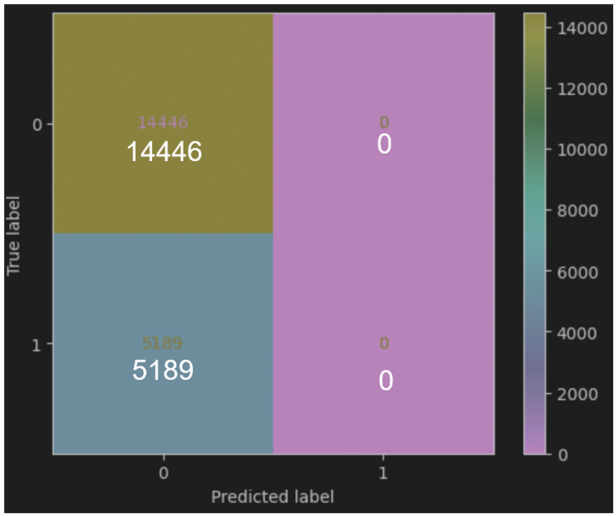

Figure 5: The confusion matrix for device location

3.3 Combined Model Effectiveness and Threat Mitigation Strategy

To assess the mitigation potential of the IZTA models against CBS authentication threats and vulnerabilities, the study adopted a quantitative evaluation model, herein referred to as the IZTA Threat Mitigation Model.

Calculating the Average Effectiveness and Ineffectiveness Rates

In this study, Accuracy determines effectiveness. Therefore, the effectiveness rate is equated with the accuracy of the two models and is thus derived from the quantitative accuracy of the two models. To determine effectiveness and ineffectiveness rate, the calculation for the combined average accuracy of the two models. Therefore the **ineffectiveness rate** is the residual of the effectiveness rate. The two indicators are

calculated as indicated under Eq. (3):

$$\begin{aligned} &\textit{Effectiveness Rate} = \textit{Models Average Accuracy} \\ &\textit{Average Accuracy} = \frac{0.8766 + 0.7357}{2} = 0.8063 \\ &\text{therefore:} \\ &\textit{Ineffectivenes Rate} = 1 - \textit{AverageAccuracy} \\ &\textit{Ineffectiveness Rate} = 1 - 0.8063 = 0.1937 \end{aligned} \tag{3}$$

Eq. (3): Average Effectiveness and Ineffectiveness Rates

The formula and calculations in Eq. (3) indicate that the IZTA models collectively mitigate approximately 80.63% of CBS authentication threats, while 19.37% may persist as residual risk even after model intervention.

3.3.1 Threat Severity before Mitigation

The Initial Base Score (IBS) represents the unmitigated severity level of a given threat prior to the application of the IZTA model. IBS values were derived from simulated attack scenarios and guided by industry frameworks such as the Common Vulnerability Scoring System (CVSS). The IBS is expressed as indicated in Eq. (4):

$$\begin{aligned} &\textit{IBS} = f\,(\textit{Threat Category, Likelihood, Potential Impact}) \\ &\text{where} \\ &\boldsymbol{IBS}\ \textit{denotes the Initial Base Score} \\ &\boldsymbol{f}\,(.)\ \textit{captures a weighted assesment of risk parameters associated with each threat type} \end{aligned} \tag{4}$$

Eq. (4): Initial Base Score Calculation

The calculation in Eq. (4) offers baseline values that act as a reference point for measuring the reduction in threat impact achieved through IZTA implementation.

3.3.2 Threat Severity after Mitigation

The Mitigated Base Score (MBS) is calculated by adjusting the IBS through the application of the IZTA model's Ineffectiveness Rate (IR), which reflects the proportion of residual threat that bypasses the model's defensive mechanisms. The MBS is computed using Eq. (5):

$$\begin{aligned} &\textit{MBS} = \textit{Initial Base Score}\,(\textit{IBS}) * \textit{Ineffectiveness Rate}\,(\textit{IR}) \\ &\text{where} \\ &\boldsymbol{MBS}\ \text{refers to the mitigated Base Score after IZTA intervention} \\ &\boldsymbol{IR}\ \text{is the Ineffectiveness Rate of the IZTA model}\ (0 \leq \textit{IR} \leq 1) \\ &\text{For example, a Brute Force attack with an IBS of 7.00 and an IR of 0.1937 yields:} \\ &\boldsymbol{MBS} = 7.00 * 0.1937 = 1.36 \end{aligned} \tag{5}$$

Eq. (5): Mitigated Base Score Calculation

The calculations in Eq. (5) illustrate the reduction in severity facilitated by the IZTA controls, confirming the model's capacity to substantially lower threat impact under operational conditions.

3.3.3 Severity Classification Thresholds

To standardize the interpretation of both IBS and MBS values, the following severity rating thresholds were employed:

i. Low severity: 0.00–3.99
ii. Medium severity: 4.00–6.99
iii. High severity: 7.00–10.00

These thresholds provide a consistent classification system for evaluating the residual risk associated with each threat vector before and after mitigation.

3.4 Practical Implications

This quantitative framework enables both theoretical validation and real-world assessment of the IZTA model's threat mitigation capabilities. By applying consistent mathematical metrics and severity classifications, the study demonstrates how machine learning–augmented security controls can substantially reduce authentication-related risks in cloud environments. The formulas also support dynamic recalculations in simulation environments, accommodating evolving threat landscapes and adaptive model training iterations as indicated in Table 3.

Table 3: IZTA threat mitigation model results

No.	Threat category	Initial base score (IBS)	IZTA ineffectiveness rate (IR)	Mitigated base score (MBS)	Severity rating
1	Brute force attacks	7.00	0.1937	1.36	Low
2	Denial of service attacks	4.30	0.1937	0.83	Low
3	Password discovery attacks	3.60	0.1937	0.70	Low
4	Social engineering attacks	3.40	0.1937	0.66	Low
5	Man-in-the-middle attacks	1.40	0.1937	0.27	Low

The analysis of Table 3 helps the study to produce the IZTA model as indicated in Fig. 6:

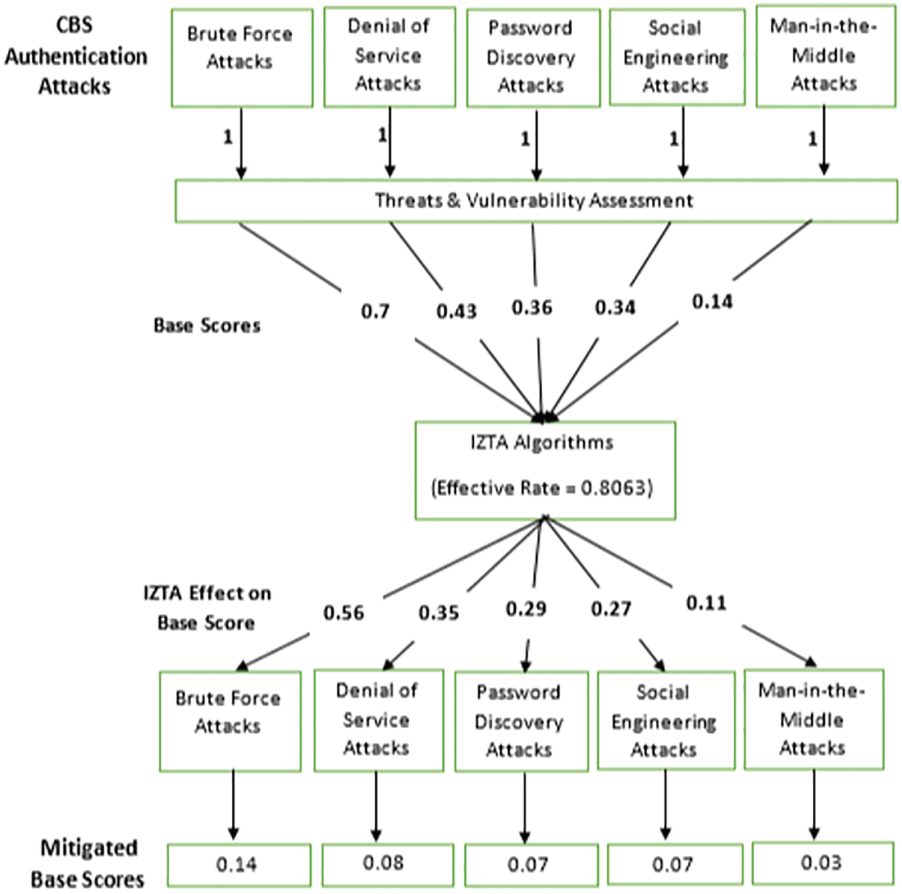

Figure 6: Visual representation of the IZTA threat mitigation model

3.5 Scenario-Based Simulation of IZTA Performance under Varying Conditions

To evaluate the robustness and adaptability of the Intelligent Zero Trust Architecture (IZTA) model, this study developed five distinct scenarios that simulate different real-world conditions affecting authentication threat mitigation in Cloud-Based Services (CBS). These simulations provide insight into the dynamic behavior of the IZTA model under varying levels of effectiveness, threat severity, and adaptive intelligence. The foundational equation for determining mitigated risk is based on the relationship indicated in Eq. (6).

$$\textit{Mitigated Base Score}\,(MBS) = \textit{Initial Base Score}\,(IBS) * \textit{Ineffectiveness Rate}\,(IR)$$

therefore (6)

$$\boldsymbol{MBS} = IBS * IR$$

Eq. (6): Foundational Equation for Determining Mitigated Risk

Eq. (6) is used by the research work to calculate different IZTA model scenarios so as to determine the effectiveness of the IZTA model in mitigating cloud-based authentication threats and vulnerabilities under different real-life scenarios.

3.5.1 Scenario 1: Increased IZTA Ineffectiveness (IR = 0.35)

This scenario models the situation where IZTA's performance declines, possibly due to adversarial adaptation, degraded model learning, or infrastructural constraints. The increase in the ineffectiveness rate to 0.35 results in higher mitigated scores for each threat, as shown in Table 4.

In Scenario 1 as highlighted by Table 4, when the ineffectiveness of IZTA is increased by increasing the values of its ineffectiveness rate (IR), there is a slight elevation in threat severity is observed, with brute force attacks approaching a medium-risk threshold, highlighting the need for continuous model tuning.

Table 4: Impact of increased IZTA ineffectiveness

Threat category	IBS	IR	MBS	Severity
Brute force attacks	7.00	0.35	2.45	Medium
Denial of service attacks	4.30	0.35	1.51	Low
Password discovery attacks	3.60	0.35	1.26	Low
Social engineering attacks	3.40	0.35	1.19	Low
Man-in-the-middle attacks	1.40	0.35	0.49	Low

3.5.2 Scenario 2: Enhanced IZTA Efficiency (IR = 0.10)

In this simulation, the IZTA model becomes more effective through optimization of its learning algorithms and contextual feature integration. The ineffectiveness rate is reduced to 0.10, reflecting heightened model responsiveness as indicated in Table 5.

Table 5: Enhanced effectiveness with reduced IR

Threat category	IBS	IR	MBS	Severity
Brute force attacks	7.00	0.10	0.70	Low
Denial of service attacks	4.30	0.10	0.43	Low
Password discovery attacks	3.60	0.10	0.36	Low
Social engineering attacks	3.40	0.10	0.34	Low
Man-in-the-middle attacks	1.40	0.10	0.14	Low

All threats remain well within the low severity bracket, indicating a strong performance from the IZTA model in a stabilized environment.

3.5.3 Scenario 3: Surge in Threat Landscape (IBS Spike)

This scenario assumes a spike in brute force attacks due to the discovery of a novel vulnerability or exploitation technique, raising the initial score from 7.00 to 9.00 while IR remains constant at 0.1937. This is as indicated by Table 6.

Table 6: Increased IBS for brute force attack

Threat category	IBS	IR	MBS	Severity
Brute force attacks	9.00	0.1937	1.74	Low
Denial of service attacks	4.30	0.1937	0.83	Low

(Continued)

Table 6 (continued)

Threat category	IBS	IR	MBS	Severity
Password discovery attacks	3.60	0.1937	0.70	Low
Social engineering attacks	3.40	0.1937	0.66	Low
Man-in-the-middle attacks	1.40	0.1937	0.27	Low

Despite the escalation in initial risk score, IZTA effectively mitigates the impact to maintain a low severity profile.

3.5.4 Scenario 4: Selective Optimization (Variable IR by Threat Type)

This scenario models adaptive tuning where different IR values are applied based on the threat category, reflecting a mature IZTA model trained to recognize and prioritize specific threats.

Table 7 indicates that customized response patterns enhance IZTA's risk-to-effort ratio, leading to more efficient security operations.

Table 7: Threat-specific IR optimization

Threat category	IBS	IR	MBS	Severity
Brute force attacks	7.00	0.12	0.84	Low
Denial of service attacks	4.30	0.18	0.77	Low
Password discovery attacks	3.60	0.15	0.54	Low
Social engineering attacks	3.40	0.20	0.68	Low
Brute force attacks	7.00	0.12	0.84	Low

3.5.5 Scenario 5: Learning over Time (Dynamic IR Reduction)

In this final scenario depicted by Table 8, IZTA's machine learning modules evolve, reducing the IR across iterations. This simulates long-term deployment with continuous learning.

Table 8: IR declines over time (brute force as example)

Iteration	IR	MBS (Brute Force)	Severity
1	0.25	1.75	Low
2	0.20	1.40	Low
3	0.15	1.05	Low
4	0.10	0.70	Low
5	0.05	0.35	Low

Table 8 indicates that progressive model refinement leads to an exponential reduction in threat severity, confirming the scalability and learning capability of IZTA.

3.5.6 Summary of Scenario Simulations

The different scenarios depicted by Tables 4–8 are summarized by the study to give an overview of scenario outcomes as indicated in Table 9.

Table 9: Overview of scenario outcomes

Scenario	Simulated condition	Risk trend	Key insight
1. Increased IR	Decreased model effectiveness	Risk increases	High-risk vectors re-emerge
2. Reduced IR	Improved model effectiveness	Risk reduces	Model achieves significant threat control
3. Increased IBS	Escalating threat landscape	Risk controlled	IZTA effectively absorbs threat surges
4. Variable IR	Adaptive threat learning	Efficient mitigation	Threat-specific responses enhance resilience
5. Learning IR (Iterative decline)	Continuous model training	Long-term reduction	Sustained learning leads to proactive defense

These scenarios demonstrate the flexibility, scalability, and learning capacity of the IZTA model under real-world authentication threat conditions. They also underscore the importance of ongoing monitoring, adaptive learning, and contextual intelligence in modern cybersecurity frameworks.

3.6 Modeling and Equation-Based Scenario Simulations

This section presents a set of mathematical scenarios simulated to evaluate the behavior of the Intelligent Zero Trust Architecture (IZTA) model under varying threat conditions and ineffectiveness rates. Each scenario applies a modified version of the base formula for calculating the Mitigated Base Score (MBS) as indicated by Eq. (7).

$$MBS = IBS * IR$$

where

MBS = Mitigated Base Score (The residual Threat severity after IZTA intervention) (7)

IBS = Initial Base Score (As measured by CVSS of threat baseline)

IR = IZTA Ineffectiveness Rate (The proportion of the threat not mitigated)

Eq. (7): Base Formula for Calculating the Mitigated Base Score.

As per the formula, Eq. (7) scenarios simulate potential variations in the security environment and system performance.

3.6.1 Scenario 1: Increased Ineffectiveness Rate (IR = 0.35)

In this scenario, the ineffectiveness rate is raised from the baseline (IR = 0.1937) to 0.35 to simulate model degradation due to emerging threat complexity or model drift. The new formula becomes:

$$MBSx_1 = IBS * 0.35$$

This leads to a higher residual threat score, especially for high-severity vectors such as brute force attacks. For example:

$MBS_{BruteForce} = 7.00 * 0.35 = 2.45$

Although still within the "Low" severity classification, such values approach the threshold of medium risk, indicating the need for model retraining or layered mitigation.

3.6.2 Scenario 2: Decreased Ineffectiveness Rate (IR = 0.10)

This scenario reflects enhanced IZTA effectiveness due to improved learning or optimization. The ineffectiveness rate is reduced to 0.10, resulting in the formula:

$MBSx_2 = IBS * 0.10$

For instance:

$MBS_{DoS} = 4.30 * 0.10 = 0.43$

This outcome indicates a significantly improved security posture, with all threats remaining well within low severity ranges, validating the IZTA's optimization benefits.

3.6.3 Scenario 3: Elevated Threat Landscape (IBS Surge)

This scenario assumes a spike in the initial threat score for Brute Force attacks due to a newly discovered exploit, increasing IBS from 7.0 to 9.0. Maintaining the original ineffectiveness rate of 0.1937, the formula becomes:

$MBSx_3 = 9.00 * 0.1937 = 1.7433$

Despite the rise in IBS, the resulting MBS still falls under low severity, demonstrating IZTA's resilience to moderate threat escalation.

3.6.4 Scenario 4: Selective Optimization per Threat Category (Adaptive IR)

In this scenario, the ineffectiveness rate is varied by threat type to simulate targeted model tuning. The adjusted formulas are as follows:

i. Brute Force Attacks: $MBS_{BF} = IBS \times 0.12$
ii. Denial of Service: $MBS_{DoS} = IBS \times 0.18$
iii. Password Discovery: $MBS_{Pwd} = IBS \times 0.15$
iv. Social Engineering: $MBS_{SE} = IBS \times 0.20$
v. Man-in-the-Middle: $MBS_{MitM} = IBS \times 0.25$

This adaptive approach demonstrates the potential of fine-grained ML tuning for different threat vectors, yielding cost-effective mitigation with minimal residual risk.

3.6.5 Scenario 5: Learning over Time (Dynamic IR Reduction)

This scenario models an iterative reduction in the ineffectiveness rate to reflect continuous learning and model enhancement over time. The ineffectiveness rate reduces linearly by 0.05 per iteration. The evolving formula is:

i. Iteration 1: MB_{S1} = IBS × 0.25
ii. Iteration 2: MB_{S2} = IBS × 0.20
iii. Iteration 3: MB_{S3} = IBS × 0.15
iv. Iteration 4: MB_{S4} = IBS × 0.10
v. Iteration 5: MB_{S5} = IBS × 0.05

This scenario illustrates how the IZTA model becomes increasingly effective over time, leading to near-zero residual threat exposure, aligning with the theoretical objectives of machine learning-based ZTA.

4 Discussion

The IZTA model in Fig. 6 indicates that the analysis of mitigated base scores (MBS) across various authentication-related threat categories provides critical insights into the practical performance of the Intelligent Zero Trust Architecture (IZTA) model. The results demonstrate that all computed MBS values fall within the "Low" severity classification (0.00–3.99) as defined by the study's standardized risk threshold. This uniformity across different threat vectors indicates a high level of consistency in the IZTA model's performance. Regardless of the initial threat magnitude, the mitigation process successfully suppresses the residual risk to manageable levels. This confirms the IZTA model's reliability and resilience under varied attack conditions. A particularly significant outcome is the model's ability to neutralize high-risk threats. For instance, Brute Force Attacks, which had an Initial Base Score (IBS) of 7.00—qualifying as a "High" severity risk—were mitigated down to an MBS of 1.36. This represents an approximate 80.5% reduction in threat intensity. Similar suppression was observed for other attack categories such as Credential Stuffing, Password Discovery Attacks, and Phishing-related intrusions. These findings underscore the IZTA model's potential to significantly reduce the threat surface in real-world cloud authentication environments.

The successful performance of the IZTA model is further attributed to its hybrid approach, integrating both behavioral and contextual trust signals. Behavioral analytics, such as keystroke dynamics, capture user interaction patterns, while contextual indicators like device location provide environmental validation. This dual-faceted trust evaluation supports the Zero Trust Architecture (ZTA) principles of continuous authentication, least privilege access, and adaptive policy enforcement. The ability of the model to dynamically interpret user legitimacy based on multiple trust layers contributes to its overall precision and effectiveness.

The consistent threat suppression achieved through this model has practical implications for cloud service providers, cybersecurity architects, and policy makers. The IZTA model not only strengthens identity verification mechanisms in real time but also contributes toward compliance with cybersecurity frameworks such as NIST's ZTA model. Moreover, its modular design and explainable machine learning foundation make it adaptable for deployment in high-risk sectors such as finance, healthcare, education, and public administration.

The quantitative application and evaluation of the Intelligent Zero Trust Architecture (IZTA) Threat Mitigation Model yielded critical findings that affirm the model's effectiveness in enhancing authentication security for Cloud-Based Services (CBS). The key results are discussed below, along with their broader implications for cybersecurity theory, practice, and policy. One of the most significant outcomes of the study is the observed uniformity in threat reduction across all evaluated attack categories. Following mitigation via the IZTA model, all threat vectors, including Brute Force, Denial of Service, Password Discovery, Social Engineering, and Man-in-the-Middle attacks, resulted in Mitigated Base Scores (MBS) that fell within the "Low" severity range. This cross-category consistency suggests a high level of generalizability and scalability of the IZTA model, reinforcing its applicability across diverse authentication environments in the cloud.

The model's capacity to suppress high-severity threats to low-impact levels further validates its robustness. For instance, Brute Force Attacks, which initially scored an IBS of 7.00 (classified as "High"), were mitigated to an MBS of 1.36 (classified as "Low"). This represents a substantial threat reduction of over 80%. Similar threat suppression was observed across other categories, including credential-based and session-layer attacks. These outcomes demonstrate that the IZTA model effectively transforms potentially catastrophic threats into manageable security events. A foundational strength of the IZTA model lies in its trust evaluation mechanism, which synergistically integrates both behavioral and contextual signals. Behavioral attributes such as keystroke dynamics provide continuous insight into user interaction patterns, while contextual factors like device location and access timing add an additional layer of dynamic verification. This dual-modality trust scoring aligns with Zero Trust principles of continuous verification, minimal privilege, and adaptive access control. Consequently, the model ensures that access decisions are evidence-based, context-aware, and responsive to evolving threat conditions.

From a practical perspective, the findings affirm that organizations can achieve higher levels of authentication assurance without imposing excessive system complexity or latency. For cybersecurity practitioners, the study provides a replicable model that integrates explainable machine learning with Zero Trust protocols. Theoretically, the study contributes to the evolving discourse on trust modeling in access control systems by demonstrating how multi-modal data streams can enhance security decision-making.

5 Conclusion

This paper presents the development, application, and evaluation of the Intelligent Zero Trust Architecture (IZTA) model designed to mitigate authentication threats in Cloud-Based Services (CBS). It outlines the model construction process, which integrates behavioral and contextual trust signals, specifically keystroke dynamics and device location, within a machine learning-driven access control framework. A six-step model development approach is adopted, beginning with threat identification and classification, and the application of an ineffectiveness rate (IR). Equations are formulated to demonstrate pre- and post-mitigation threat scores, and visualizations are used to present comparative severity ratings across threat vectors. The quantitative implementation showed that the IZTA model consistently reduced threat severity across all evaluated categories, transforming high-risk threats (e.g., brute force attacks) into low-severity risks. Findings from this study demonstrate the synergistic value of combining behavioral and contextual authentication signals. By leveraging interpretable machine learning (specifically binary logistic regression), the IZTA model ensured transparent decision-making while aligning with Zero Trust principles such as continuous validation and policy enforcement.

The study recommends that moving forward, organizations begin with interpretable models such as logistic regression for initial behavioral modeling, given their ease of implementation and transparency. Over time, however, more advanced and adaptive methods should be introduced to improve threat mitigation accuracy and reduce ineffectiveness rates. These may include the use of ensemble machine learning models like Random Forests and Support Vector Machines, as well as advanced strategies such as trust signal fusion, risk-adaptive scoring, and behavior-based anomaly detection. Incorporating these enhancements will improve model precision, reduce false positives, and enable real-time, intelligent decision-making in authentication workflows within CBS environments. These recommendations advocate for a proactive, data-driven, and layered security strategy centered on Zero Trust principles. They emphasize the need for both technical precision and adaptive policy mechanisms to ensure resilient, scalable, and intelligent authentication systems capable of withstanding evolving threat landscapes in cloud-based infrastructures.

For future research, organizations should experiment with more sophisticated machine learning architectures such as Support Vector Machines (SVMs), Random Forests, and Deep Learning models for

enhanced performance and scalability. Furthermore, the use of federated learning approaches can enable distributed training of IZTA models across multiple cloud nodes without compromising user data privacy—a critical consideration in modern security practices. Incorporating trust signal fusion techniques, adaptive risk thresholds, and confidence-based decision mechanisms may also reduce false positives and improve the model's reliability in production settings. Future work should also prioritize real-world pilot implementations of IZTA models within operational cloud environments to observe system behavior under live traffic and potential attack conditions. This would allow researchers to refine the models based on actual user interaction patterns and attack vectors encountered in practice. These future research directions emphasize the need for continued innovation in intelligent cybersecurity design. By integrating automation, signal diversity, adaptive learning, and real-world deployment, future studies can build upon the foundation established in this thesis and contribute to the development of resilient, intelligent authentication systems for the next generation of cloud computing environments.

Acknowledgement: We wish to acknowledge the Department of Information Technology, Kibabii University, for allowing us to carry out this study.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to this paper as follows: Study Conceptualization, Victor Otieno Mony, Anselemo Peters Ikoha, Roselida O. Maroko, Model Development, Victor Otieno Mony, Model Equations, Victor Otieno Mony, Roselida O. Maroko, Results Analysis, Victor Otieno Mony, Results Discussion & Presentation, Victor Otieno Mony, Anselemo Peters Ikoha, Roselida O. Maroko. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article. Further, the datasets used in this study are available online. The Device Location dataset is available at: https://www.kaggle.com/datasets/wisam1985/location-intelligence-for-cybersecurity-2025, while the Device Location Datasets are available at: https://www.kaggle.com/datasets/carnegiecylab/keystroke-dynamics-benchmark-data-set (accessed on 26 August 2025).

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Mattsson U. Zero trust architecture. In: Mattsson U, editor. Controlling privacy and the use of data assets-volume 1. Abingdon, UK: Talylor Francis Group; 2022. p. 127–34.
2. Phiayura P, Teerakanok S. A comprehensive framework for migrating to zero trust architecture. IEEE Access. 2023;11(6):19487–511. doi:10.1109/access.2023.3248622.
3. Kirti. Exploring cloud security challenges: an in-depth analysis of emerging threats and mitigation strategies. In: 2025 3rd International Conference on Disruptive Technologies (ICDT); 2025 Mar 7–8; Greater Noida, India. doi:10.1109/ICDT63985.2025.10986561.
4. Joshi M, Budhani S, Tewari N, Prakash S. Analytical review of data security in cloud computing. In: 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM); 2021 Apr 28–30; London, UK. doi:10.1109/iciem51511.2021.9445355.
5. Alotaibi AF, Alzain MA, Masud M, Jhanjhi NZ. A comprehensive survey on security threats and countermeasures of cloud computing environment. Turk J Comput Math Educ. 2021;12(9):1978–90.
6. Abdullahi AD, Dargahi T, Hammoudeh M. Poster: continuous authentication in highly connected 6G-enabled transportation systems. In: 2023 IEEE Vehicular Networking Conference (VNC); 2023 Apr 26–28; Istanbul, Türkiye. doi:10.1109/VNC57357.2023.10136342.

7. Gollmann D. Authentication, Authorisation & Accountability (AAA) knowledge area issue. Bristol, UK: The Cyber Security Body of Knowledge; 2019.
8. Krishnamoorthy R, Arun S, Sujitha N, Vijayalakshmi KM, Karthiga S, Thiagarajan R. Proposal of HMAC based protocol for message authenication in kerberos authentication protocol. In: 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS); 2022 Feb 23–25; Coimbatore, India. doi:10.1109/ICAIS53314.2022.9742992.
9. Priyadharshini S, Rajmohan R. Analysis on database security model against NOSQL injection. Int J Sci Res Comput Sci Eng Inf Technol. 2017;2(2):2456–3307.
10. Dostalek L, Safarik J. Strong password authentication with AKA authentication mechanism. In: 2017 International Conference on Applied Electronics (AE); 2017 Sep 5–6; Pilsen, Czech Republic.
11. Akram SV, Joshi SK, Deorari R. Web application based authentication system. In: 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC); 2022 Nov 18–19; Bengaluru, India. doi:10.1109/IIHC55949.2022.10059984.
12. Raheman F, Bhagat T, Vermeulen B, Van Daele P. Will zero vulnerability computing (ZVC) ever be possible? Testing the hypothesis. Future Internet. 2022;14(8):238. doi:10.3390/fi14080238.
13. Abdulsalam YS, Hedabou M. Security and privacy in cloud computing: technical review. Future Internet. 2022;14(1):11. doi:10.3390/fi14010011.
14. Ahmadi S. Zero trust architecture in cloud networks: application, challenges and future opportunities. J Eng Res Rep. 2024;26(2):215–28. doi:10.9734/jerr/2024/v26i21083.
15. Alawneh M, Abbadi IM. Integrating trusted computing mechanisms with trust models to achieve zero trust principles. In: 2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS); 2022 Nov 29–Dec 1; Milan, Italy. doi:10.1109/iotsms58070.2022.10062269.
16. Kancherla VM. The next-generation cloud security model: AI-powered zero trust and adaptive threat prevention. Int J Emerg Trends Comput Sci Inf Technol. 2025;6:82–90. doi:10.63282/3050-9246.ijetcsit-v6i1p110.
17. Zhou L, Song X, Yao G, Wang H, Li J, Liu S, et al. Intelligent sensing terminal distributed computing architecture of IoT for EMS. In: 2023 IEEE 14th International Symposium on Power Electronics for Distributed Generation Systems (PEDG); 2023 Jun 9–12; Shanghai, China. doi:10.1109/PEDG56097.2023.10215140.
18. Wang Z, Yu X, Xue P, Qu Y, Ju L. Research on medical security system based on zero trust. Sensors. 2023;23(7):3774. doi:10.3390/s23073774.
19. Wei Q. Analysis of the role of computer big data and cloud computing in information security. In: 2023 International Conference on Networking, Informatics and Computing (ICNETIC); 2023 May 29–31; Palermo, Italy. doi:10.1109/ICNETIC59568.2023.00031.
20. Tiwari A, Patel PJ, Sharma DP. Vulnerability assessment and penetration testing approach towards cloud-based application and related services. Int J Sci Res Sci Eng Technol. 2021;2021:395–403. doi:10.32628/ijsrset218346.
21. Tsai M, Lee S, Shieh SW. Strategy for implementing of zero trust architecture. IEEE Trans Reliab. 2024;73(1):93–100. doi:10.1109/TR.2023.3345665.