Int. j. adv. multidisc. res. stud. 2026; 6(4):226-236

Received: 17-05-2026
Accepted: 27-06-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Secure Access Control for Multi-Tenant Cloud Systems Using a Behavioral Zero-Trust Framework with Machine Learning and Blockchain-Based Auditing

[1] Musab Umair Malik, [2] Muhammad Faisal Shafiq, [3] Muhammad Naveed Sajjad, [4] Muhammad Irshad

[1] Alinma Bank, Riyadh, Saudi Arabia
[2] Sr. Security Analyst, Lucid Motors, Riyadh, Saudi Arabia
[3] Sr. Cybersecurity Consultant, Yanal Finance, Riyadh, Saudi Arabia
[4] Cybersecurity GRC Consultant, RMG Company, Riyadh, Saudi Arabia

Corresponding Author: **Musab Umair Malik**

Abstract

The expansion and emergence of multi-tenant cloud platforms have posed significant challenges for securing and maintaining reliable access control, especially when considering how users behave at different times and how cyber threats are constantly evolving. Role-based access control and attribute-based access (ABAC) are examples of traditional access control models that fail to be flexible enough to identify and block unauthorized activities and cross-tenant attacks in current cloud settings. To address these limitations, this study suggests a Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC), which establishes the integration of 3 modules in one unified framework: Machine learning based behavioral analytics, Zero-trust policy enforcement, and Blockchain based auditing. While the framework uses a behavioural- anomaly detection to produce risk-based access decisions, a zero-trust mechanism dynamically applies access policies according to pre-defined thresholds. Furthermore, a blockchain-based audit layer provides secure and tamper-proof access capability events. Multiple real-world cybersecurity datasets, such as the LANL authentication dataset, UNSW-NB15 and CICIDS2017, are utilized to assess the effectiveness of the proposed framework. Experimental results clearly show that the proposed XGBoost can achieve good detection performance with F1-scores near to 98.0% on LANL and 95.5% on UNSW-NB15 and up to 99.9% on CICIDS2017 data set, while its inference latency is low, typically from 0.002–0.005 ms per sample. In addition, there is minimal computation overhead of the audit logging, making it a real-time solution. The proposed approach provides a scalable and practical solution to improve tenant isolation, improve access control and develop trust in cloud environments by providing multi-tenancy security.

Keywords: Multi-Tenant Cloud Security, Zero-Trust Architecture, Behavioral Anomaly Detection, Machine Learning, Access Control, Blockchain Auditing, Intrusion Detection

1. Introduction

Cloud computing has revolutionized how organizations deploy and manage digital services, with a surge in both adoption and popularity. Modern cloud applications increasingly rely on multi-tenant architecture, in which physical and virtual resources are shared by multiple users or organizations while their resources are logistically separated. This architecture offers efficient resource utilization, scalability, and cost savings, making it the preferred choice for Software-as-a-Service (SaaS) applications and enterprise cloud deployments. Multi-tenant applications, however, can present a host of security challenges, especially in the realm of identity management, tenant isolation, and enforcement of access controls (Waller *et al*., 2011 [26]; Zhou *et al*., 2010 [28]; Singh & Chatterjee, 2021). Thus, it is important to establish secure and reliable access control mechanisms that become a basic need to secure critical workloads into cloud infrastructures and protect sensitive information or to maintain the integrity in the system (Barka & Sandhu, 2000) [4].

Security in distributed computing environments heavily relies on access control mechanisms. In order to control the access permissions and enforce authorization policies, the traditional access control methods such as Rolebased Access Control

(RBAC) and Attribute Based Access Control (ABAC) had been widely used in enterprise systems (Jin *et al*., 2012; Hu *et al*., 2014; Sandhu *et al*., 1996) [14, 13, 21]. RBAC having the roles assigned to users and permission to the roles makes permission management easy, but ABAC is more flexible as it allows incorporating user identity, device type, environment, etc. (Jin *et al*., 2012; Hu *et al*., 2014; Servos & Osborn, 2017) [14, 13, 23]. Although these models work well in traditional infrastructures, they have several drawbacks associated with dynamic cloud infrastructures, especially in a multi-tenant setting, where fast changes in access patterns are present and context awareness is needed to identify abnormal access patterns (Ferraiolo *et al*., 2007; Zhou *et al*., 2010) [11, 28]. Static Policy enforcement and limited behavioral analysis can cause vulnerabilities and get permissive behavior across tenants.

A major security concern with multi-tenant systems is the potential of cross-tenant attacks, which involve an adversary entering into resources of another tenant's system as a result of vulnerabilities with authentication or authorization. Traditional types of attacks include things like credential compromise, lateral movement or privilege escalation on shared infrastructures (Waller *et al*., 2011; Singer & Friedman, 2013; Ferrag *et al*., 2020) [26, 24, 10]. Lateral movement attacks are especially threatening because a bad actor, once they have initial access to a system, can gradually move throughout the network and gain access to further systems through the use of legitimate authentication methods (Ring *et al*., 2019; Ferrag *et al*., 2020) [19, 10]. However, Static authorization policies are insufficient for detecting such behaviors in dynamic cloud environments; continuous monitoring of authentication events and system logs is essential (Kent & Souppaya, 2006; Ring *et al*., 2019) [16, 19].

To address these constraints, some recent research has focused on how to incorporate behavioral analytics and machine-learning algorithms in cybersecurity systems for improved anomaly detection and adaptive access control. Machine learning algorithms can be used to process large amounts of authentication logs and network traffic data and detect suspicious patterns that could be indicative of compromised accounts or unauthorized access attempts (Sommer & Paxson, 2010; Buczak & Guven, 2016; Ahmad *et al*., 2021) [25, 5, 1]. Behavioral anomaly detection techniques can be used to learn normal user access behaviours and pinpoint out-of-control access times, unusual use of devices or sporadic access frequencies (Buczak & Guven, 2016 [5]; Ahmed *et al*., 2016 [2]; Ahmed *et al*., 2020; Ahmad *et al*., 2021 [1]). These methodologies work especially well in cloud infrastructures where vast amounts of integrity events and system log information can be used to build predictive security models.

Another crucial paradigm gaining significant attention to-date in contemporary cybersecurity research is Zero-Trust Architecture (ZTA) which assumes that nothing inside or outside the network is to be trusted by default (Rose *et al*., 2020 [20]; Kindervag, 2010 [17]; NIST, 2020). In contrast to traditional perimeter security approaches, Zero-Trust security necessities continuous verification of various pieces of information (such as identity, device integrity, and contextual factors) before allowing access to resources. This works particularly well in a multi-tenant cloud scenario where resources are distributed across different tenants and access is requested from various resources and devices (Rose *et al*., 2020) [20]. With the integration of context correlated with behavioral risk, Zero-Trust policies can be dynamically configured and unauthenticated interactions between tenants prevented.

Dynamic authorization mechanisms are important, so is the integrity and traceability of access logs for auditing purposes and to hold individuals accountable for their actions, as well as to assist forensic analysis. Standard logging systems can be subject to manipulation or unauthorized changes, potentially undermining audit log accuracy. To solve this problem, researchers have suggested that blockchain technology can be integrated into security systems allowing tamper resistant and distributed logging (Zyskind *et al*., 2015; Dorri *et al*., 2016; Zhang *et al*., 2018) [29, 9, 27]. Blockchain-based auditing produces cryptographic hashes of security events, which are recorded on a blockchain, making it impossible to modify access logs without it being identified. In multi-tenant cloud setups where various parties may need clear, auditable logs, these immutable logging features prove useful.

While there are numerous studies that research different aspects of cloud security, the studies that directly deal with anomaly detection, zero-trust policies and blockchain auditing of multi-tenant systems are often studied separately. Moreover, the synthetic datasets or limited experimentation were tried on several proposed models, which makes them less practical to be used in the actual enterprise environments (Sommer & Paxson, 2010; Ahmad *et al*., 2021; Ferrag *et al*., 2020) [25, 1, 10]. The datasets of large-scale authentication (such as the Los Alamos National Laboratory cybersecurity dataset) offer a chance to test access control systems with enterprise-level authentication patterns and interactions (Kent & Souppaya, 2006; Waller *et al*., 2011; Ring *et al*., 2019) [16, 26, 19].

This study aims to propose a Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC) for Multi-Tenanted Cloud System to overcome these drawbacks. The suggested architecture combines machine learning algorithms for behavioral analytics and anomaly detection with a zero-trust policy enforcement mechanism for dynamic authorization and blockchain-based auditing for robust and tamper-proof event processing and record keeping. The proposed framework brings these components together under the umbrella of a unified architecture to boost tenant isolation and real-time threat detection unlike existing approaches that individualize them. Its performance is tested on the effectiveness of the framework by employing multiple real life cybersecurity datasets to illustrate the capability in detecting anomalous access pattern without compromising the efficiency and security of the access control.

The main contributions of this study are:

1. A unified SB-ZTAC framework integrating behavioral analytics, zero-trust, and blockchain auditing.
2. A machine learning-based behavioral risk scoring mechanism for adaptive access control.
3. Formal verification of tenant isolation policies using SMT-based methods.
4. Comprehensive evaluation across LANL, UNSW-NB15,

and CICIDS2017 datasets.
5. Performance analysis of blockchain-based audit overhead in real-time systems.

2. Related Work

2.1 Traditional Access Control Models

Access control has always been a fundamental component of information security systems. One of the most widely used and accepted is the Role-Based Access Control model (RBAC), which makes it easier to manage authorizations by assigning them to roles instead of users. In the case of RBAC systems, users gain access to resources by virtue of the roles assigned to them and this facilitates the management of environments of large-scale enterprises (Sandhu *et al*., 1996, Ferraiolo *et al*., 2007) [21, 11]. The use of RBAC in various organizational systems has been successful due to its simplicity, scalability, and structured approach to permission management.

Some of the traditional RBAC models, however, turn out to be inadequate in dynamic environments like cloud computing systems, where contextual information is significant for security decisions. To resolve this restriction, Attribute-Based Access Control (ABAC) was developed which uses several attributes to determine access (Hu *et al*., 2014; Servos & Osborn, 2017) [13, 23]. ABAC supports access fine graining and run-time decision making making it more appropriate to use in the distributed systems scenario than static role-based approaches do.

Though RBAC and ABAC have their benefits, both of them come with their share of difficulties, especially in today's cloud-based environment. Large scale multi-tenant systems state that access patterns often vary and policies should evolve over time to take care of the changing security scenario. While static authorization models are great, they are not necessarily behavior-aware and don't provide real-time risk assessments, which can result in unauthorized access or privilege escalation attacks (Zhang *et al*., 2020; Singh & Chatterjee, 2021). As such, more recently, adaptive and behavior-aware access control mechanisms have been considered that can overcome such limitations.

$$q_i = \sum_j W_{ij}(G) I_j \tag{1}$$

Where i, j is the pixel index, weight W_{ij} determined by guided graph G, which is completely independent from the input image.

2.2 Security Challenges in Multi-Tenant Systems

Multi-Tenant Cloud provides the ability to provide multiple organizations with an ability to share computing resources while providing a logic separation between tenants. This architecture provides better utilization of resources and lowers the costs of running, but it adds a number of security issues concerning tenant isolation, identity management, and access control enforcement (Zhou *et al*., 2010; Almorsy *et al*., 2016) [28, 3]. In those types of environments, some weaknesses in authentication systems or access control policies can give hackers access to resources associated with other tenants.

The cross-tenant attack is one of the most critical threats in multi-tenant environments where a malicious user takes advantage of flaws in the system isolation of multi-tenanted software and accesses some service or data to which it isn't entitled from another tenant. These attacks can be carried out via stolen credentials, poor access management policies, and weaknesses in shared infrastructure elements (Singer & Friedman, 2013 [24]; Zhang *et al*., 2020). Attacks may also make a lateral move, which is where attacks proceed and gradually start increasing privileges after gaining access to the first interconnected system (Ring *et al*., 2019) [19].

The complexity of distributed cloud infrastructures becomes another challenge due to the number of managed identities and permissions. Modern cloud platforms frequently end up with multiple authentication services, APIs, and microservices, making it easy to mess up configuration and policies (Singh & Chatterjee, 2021). Consequently, traditional access control mechanisms might not be enough to ensure that tenants are secure and segregated in a dynamic multi-tenant environment and that security is monitored in real-time.

2.3 AI-Based Security Systems

Traditional access controls approaches were unable to resolve some problems which made research into using machine learning technique and methods for security monitoring and detection of anomalies. Machine learning algorithms can be used to analyze large amounts of account authentication logs and network traffic information to detect suspicious activity that may be a sign of a compromised account or malicious behavior (Sommer & Paxson, 2010; Buczak & Guven, 2016) [25, 5].

Many intrusion detection and behavior analysis techniques have been researched in the context of supervised and unsupervised learning. Random Forest, XGBoost, and deep neural networks are algorithms that have shown excellent results in the context of anomaly detection in cybersecurity data sets (Ferrag *et al*., 2020; Ahmad *et al*., 2021) [10, 1]. These models can be trained with the historical data of previous attempts to recognize normal behavior, requiring the identification of any logins outside the norm, such as logins at strange, irregular times, the use of an unusual device, or other frequencies of logins that aren't normal.

More recently, research has been conducted on how to incorporate the use of machine learning techniques in cloud security architectures to achieve adaptive access control functions. AI-powered security systems can use behavioral analytics in authorisation, making it possible to adapt access policies dynamically and also identify in real-time suspicious actions (Ahmed *et al*., 2016; Ahmad *et al*., 2021) [2, 1]. These are especially beneficial when dealing with cloud environments, where vast amounts of log information can help achieve more accurate threat detection.

2.4 Blockchain in Access Control

Besides anomaly detection mechanisms, the integrity and trustworthiness of security logs and audit trails are fundamental to support accountability and transparency in cloud systems. In traditional logging systems, the storage of logs is centralized, which can open the door to potential tampering or unauthorized changes. To address this restriction, it has been suggested that auditing can be implemented via blockchain technology so it can be tamper resistant and decentralised (Zyskind *et al*., 2015 [29]; Dorri *et al*., 2017).

Security frameworks based on blockchain can be used to securely store cryptographic hash representations of system events or access transactions. Blockchain ledgers are

distributed and immutable, making it easy to detect any changes in previously recorded information (Casino *et al*., 2019) [6]. The immutability of blockchain suits this property, making it ideal for secure audit trails in multi-tenant environments where various stakeholders need logging with transparency and verifiability.

However, several studies have discussed access control frameworks for cloud computing and IoT by utilizing the Blockchain. These are all efforts to enhance trust management and decentralized policy enforcement, and to minimize centralized authorities (Dorri *et al*., 2017; Zhang *et al*., 2018 [27]). However, it is crucial to consider the potential for scalability and latency issues in the application of blockchain to real-time cloud access control systems.

2.5 Research Gaps

While substantial research exists on topics like access control models, behavioural anomaly detection, blockchain-based auditing systems, each of these works addresses just one or another independent of each other. Traditional access control systems do not have behavioral sensitivity and machine learning-based systems are not necessarily used within authorization systems. Likewise, the typical issue raised by blockchain solutions is about the integrity of the audit rather than the enforcement of dynamic access control. As a result, an integrated security framework that brings together behavioral analytics, zero-trust authorization policies and immutable auditing capability in a single, purpose-built architecture for dealing with the unique nature of multi-tenant environments in the cloud has not yet emerged. To facilitate real-time anomaly detection, secure and transparent access control and enhance tenant isolation abilities in modern cloud-based infrastructure, this gap has to be addressed.

3. Methodology

In this study, a Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC) is proposed to improve security in multi-tenant cloud environments. It combines behavioral analytics, zero-trust and blockchain-based auditing into a single architecture to ensure adaptive, context-aware and tamper-resistant access control.

3.1 Framework Overview

The SB-ZTAC framework is divided into four main modules: (1) Identity Verification Layer, (2) Behavioral Risk Analysis Engine, (3) Zero-Trust Policy Engine and (4) Blockchain-Based Audit Module. All these components together can offer secure authentication, adaptive access authorization, and tamper-proof access events auditing.

Every access request goes through a pipeline of structured processing steps, whereby identity checking, behavioural risk assessment and policy enforcement are done before the final decision is logged into the audit layer. This design is context-aware and continually validated to abide by ZT principles for access control decisions. The proposed SB-ZTAC framework is presented with overall architecture, see Fig 1.

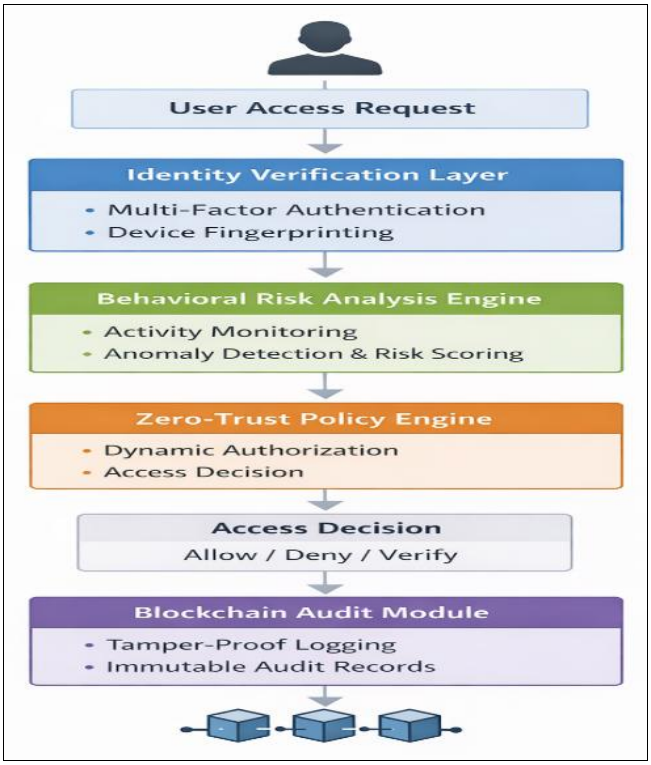

Fig 1: Architecture of the proposed Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC), illustrating identity verification, behavioral risk analysis, zero-trust decision-making, and blockchain-based auditing

3.2 Identity Verification Layer

The Identity Verification Layer provides authentication services that ensure that users can gain access to system resources. This layer also includes multi-factor authentication (MFA) mechanisms that demand users to give multiple types of verification, such as a password, biometric information or one-time authentication codes. MFA drastically diminishes the risk of credential compromise (Rose *et al*., 2020) [20].

The framework also includes device fingerprinting techniques to help identify and validate devices accessing the system as well as authentication. The device fingerprinting gathers information like browser information, hardware information, operating system and IP address which can help build an individual profile for every device. The system can be compared to the existing profiles of the device in the database and identify an anomaly when accessing the device, thereby alerting users of any suspicious logins (Ahmad *et al*., 2021) [1].

3.3 Behavioral Risk Analysis Engine

The proposed framework includes the Behavioral Risk Analysis Engine as an essential element, which aims at identifying abnormal usage patterns, based on machine learning methods. This engine examines several characteristics of authentication logs and network activity: login frequency, device changes, unusual login times and network traffic patterns.

Machine learning algorithms like random forest, XGBoost, and neural networks are trained to learn the normal behavior patterns and detect deviations that might signal fraudulent activity (Buczak & Guven, 2016; Ferrag *et al*., 2020) [5, 10]. Such as, if someone tries to log in from an unusual geographical location or attempts to log in more frequently than usual, the login may be considered as high risk behavior.

The behavioral analysis results in a risk score that is the probability that a particular access will be malicious. This risk score is updated in real time based on the user activity and it is used by the authorization engine to decide access.

3.4 Zero-Trust Policy Engine

The Zero-Trust Policy Engine is responsible for making dynamic decisions on access, based on the principles of Zero-Trust Architecture (ZTA), which holds that nothing should be trusted by default, not even users or devices (Rose *et al*., 2020) [20]. Unlike traditional access control models that rely on predefined roles or attributes, the zero-trust concept uses contextual information and behavioral risk scores to evaluate each access request in real time.

The policy engine invokes a set of rules to consider several contextual attributes such as user identity, device integrity, session context and dynamically calculated risk scores. Access is only allowed if all the security conditions are met, enforcing the authorization policies. The method can be used for adaptive authorization, which means access rights can be dynamically adjusted based on the changing security environment and contextual risk factors (Rose *et al*., 2020; He *et al*., 2022) [20, 12].

The zero-trust model is an effective approach to ensure that access is always authenticated and trusted, which dramatically lowers the likelihood of unauthorized access or attacks across tenants in multi-tenant environments.

3.5 Blockchain-Based Audit Layer

The Blockchain Based Audit Layer offers a secure, tamper-proof way of recording access events. Traditional logging systems are open to manipulation which may affect the integrity of audit trails. The solution to this limitation is to incorporate the blockchain technology in the proposed framework, which guarantees the immutability and transparency of access logs (Zyskind *et al*., 2015; Casino *et al*., 2019) [29, 6].

However, blockchain systems are known to have performance issues, so the framework uses a hybrid approach and splits out the real-time decision making process from the audit storage. Access control decisions are made instantly in the off-chain layer with minimal latency using the zero-trust engine. The on-chain layer stores access logs in a cryptographic hash, which is then recorded on the blockchain at regular intervals, ensuring security and verification.

This hybrid solution keeps the system performing well and maintains integrity and traceability of access events. The framework thus facilitates efficient real-time access control and forensics analysis and compliance auditing.

3.6 Dataset

This study leverages several of the public cybersecurity datasets containing real-world authentication behavior and network traffic patterns to assess the effectiveness of the proposed Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC). Multiple datasets are used to evaluate the model comprehensively for various attack scenarios, and to improve the model's generalizability.

In this research, three well-known datasets are employed, which are the Los Alamos National Laboratory (LANL) authentication dataset, the UNSW-NB15 dataset and the CICIDS2017 dataset.

The LANL authentication dataset consists of large scale enterprise authentication logs of user–computer interactions over time. Contains more than 708 million authentication events across 9 consecutive months including attributes like user ID, computer ID and time. This data set is ideal for modeling user behavior and identifying unusual user behavior, such as enterprise network lateral movement (Kent, 2014; Ring *et al*., 2019) [15, 19].

The UNSW-NB15 is a modern network intrusion detection dataset containing both normal and malicious traffic from various types of attack including denial of service, exploits and reconnaissance attacks. It has 49 features extracted from network traffic, which is suitable for network-based attack scenarios (Moustafa & Slay, 2015) to evaluate anomaly detection models.

Another popular benchmark dataset is CICIDS2017, which is a simulated dataset for realistic cyberattack scenarios such as infiltration attack, botnets, distributed denial-of-service (DDoS) and brute-force attacks. It is able to collect detailed network flow data, and generate labeled data for benign and malicious activities (Sharafaldin *et al*., 2018).

In multi-tenant systems, securing access is a crucial concern that involves two important factors: user behavior anomalies and network-level threats. This study aims to integrate authentication logs with network intrusion datasets to comprehensively assess the proposed framework in both areas.

3.7 Data Preprocessing

The datasets go through data pre-processing to guarantee quality and usefulness before being utilized with the machine learning models. The preprocessing pipeline comprises three stages: Data cleaning, feature extraction and data normalization.

3.7.1 Data Cleaning

The data is initially cleaned, eliminating incomplete or inconsistent records, addressing missing data, and selecting relevant features. There are no duplicate entries and corrupted logs which ensure data integrity.

3.7.2 Feature Extraction

Authentication logs and network traffic data is used to identify relevant features to observe user behavior and access patterns. These factors include logon frequency, session length, device consistency, access time, source and destination identification and failed logon attempts. The features are chosen because they are effective indicators of anomalous behavior and potential security threats (Ahmed *et al*., 2016; Buczak & Guven, 2016) [2, 5].

3.7.3 Data Normalization

The numerical features are scaled using standard numerical scaling techniques to enhance machine learning model performance. This helps to ensure that each feature will have equal influence on the model, and will not be weighted by features that have higher numerical ranges.

Categorical variables are encoded using the proper encoding technique (one-hot encoding or label encoding based on the model requirements).

3.8 Mapping LANL Dataset to Multi-Tenant Cloud Environments

The LANL data set was designed for enterprise networks, and it needs to be mapped to the multi-tenant cloud context. This mapping allows for the realistic scenario of cloud-based access control to be represented by the dataset.

Each user ID in the dataset is considered a user that belongs to a tenant, and each computer ID is associated with a cloud resource (such as a virtual machine, microservice, or container instance). These resources are accessed by authentication events.

In addition, the authentication events are chained together to create a user behavior over time which can be used to detect behavior with repeated access attempts, unusual authentication sequences, or abnormal transitions between resources. This mapping allows simulating cross-tenant access attempts and lateral movement attacks, which are a big concern in multi-tenant environments.

3.9 Machine Learning Model Implementation

For detecting behavioral anomalies, this study uses multiple machine learning models such as Random Forest, XGBoost, and neural networks. These models are trained using labeled datasets and are used to find normal and abnormal access. A behavioral risk score is computed for each model using an access request prediction generated by each model. This risk score will then be fed into the zero-trust policy engine and used to make dynamic and context-aware access control decisions.

4. System Architecture

The Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC) is a proposed architecture that will be scalable and secure for enforcing access control in multi-tenant cloud environments. The architecture is designed to enable a unified framework that combines identity verification, behavioral risk analysis, zero-trust authorization and blockchain auditing capabilities to deliver context-aware and dynamic access decisions.

The overall architecture is made up of the following components: User Interface, Authentication Server, Behavioral Risk Engine, Zero-Trust Policy Engine, and Blockchain-Based Audit Layer. The components are chained together so that every access request is analyzed in real time.

To make any request to access, the user will enter through the User Interface, the gateway to all the system's interactions. This request is then passed to the Authentication Server where the user's identity is confirmed with the support of multiple factor authentication and fingerprinting methods. This helps to prevent unauthorized users from advancing any further in the system.

Upon successful authentication, the request is then passed on to the Behavioral Risk Analysis Engine that is used to assess the request using both historical and real-time behavioral information. The engine is used to analyze various characteristics: login frequency, consistency of devices, access timing, network characteristics and more. Machine learning algorithms such as Random Forest and gradient boosting are used to calculate a risk score that indicates the probability of malicious activity (Buczak & Guven, 2016; Ferrag *et al*., 2020) [5, 10].

The computed risk score is then sent to the Zero-Trust Policy Engine, the ultimate decision-making element in the framework. The Zero-Trust model is followed by the engine, which means that no implicit trust is made, and each request is evaluated separately. Decisions on authorization are made on the basis of the verification of identity, the level of trust of the device, contextual properties, and the analysis of behavior risk. Access will be granted only when all pre-defined security policies are met, otherwise access will be denied or flagged to be further checked (Rose *et al*., 2020; Sarkar *et al*., 2022) [20, 22].

After the decision is made, this result is recorded in the Blockchain-Based Audit Layer. The framework does not store full logs in the blockchain but rather a cryptographic hash of access logs is periodically written to the blockchain. This helps to keep the audit records immutable and consistent, and also reduces the performance overhead (Casino *et al*., 2019 [6]; Dorri *et al*., 2017).

The system architecture features scalability and real-time deployment capability in multi-tenant cloud setups. All the components function independently and share information via clearly defined interfaces, enabling efficient processing of access requests. This modular architecture allows scaling and updating of identity verification, behavioural analysis, policy enforcement and audit logging without affecting the whole system. This gives the framework high-performance and security guarantees, making it suitable for dynamic cloud environments.

5. Formal Verification and Security Analysis

The proposed SB-ZTAC framework is robust and correct through formal verification techniques to validate access control policy enforcement, especially to ensure that it does not allow cross-tenant access violations. Formal methods give mathematical assurances that a security policy is properly enforced and that, with specified system conditions, no unauthorized access is possible (Clarke *et al*., 1999) [7].

This study defines tenant isolation as a security property that ensures any tenant that accesses a resource cannot access any resource from another tenant without explicit authorization. This property can be represented with logical constraints below:

"If " Tenant_A≠Tenant_B⇒Access=Denied

This rule is a basic one for multi-tenant applications, where tenant isolation is critical to avoid data leakage and unauthorized interactions among tenants.

To ensure that the policy is correct, it is modeled using formal logic, and evaluated using various tools, including the Z3 SMT solver, which is generally adopted to verify the logical policy constraints in the security systems (De Moura & Bjørner, 2008) [8]. The user identity, user association to tenant, resource ownership and conditions of access are represented as variables in the system. Constraints are then added in place to only allow access when the user's tenant matches the resource's tenant, or is allowed by explicit authorization rules that allow cross-tenant access.

Apart from logical verification, Petri Nets can also be used conceptually to model the dynamic behaviour of the system and analyse the possible state transitions which can occur in the access control process. Petri Nets are a graphical and mathematical model of system work flow, allowing the identification of potential security violations or unintended access paths (Murata, 1989) [18]. Modeling authentication,

risk evaluation, and authorization as sequential transitions makes it possible to ensure that no unauthorized state transitions enable cross-tenant access.

The formal verification process also takes into account possible attack scenarios formulated in the threat model. For example, if someone is discovered to be using a stolen credential, the system makes sure that the risk engine's detection of the behavior affects the authorization decision, and prevents access even with a valid credential. For a similar reason, in lateral movement situations the system will check whether access policies prevent unauthorized access to resources on different tenants.

The proposed framework uses formal verification techniques to ensure that the policy is correct and that it is enforced appropriately. This not only improves the reliability of the access control system, but also makes it more credible in practical applications where any proven security properties are crucial for compliance and trust.

6. Experiments

The experimental setup aims at testing and assessing the performance and effectiveness of the proposed Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC) in the context of multi-tenant cloud environments with the purpose of detecting access behaviors that are anomalous and enforcing secure authorization policies. It is implemented in a simulated cloud environment with machine learning models, real-world cybersecurity datasets and blockchain based auditing mechanism.

The experiments are all implemented in the Python programming language, which offers flexibility and scalability in data preprocessing, model building, and evaluation. The TensorFlow framework is used to implement the machine learning models, providing efficient training and deployment of traditional and deep learning models. TensorFlow is especially well suited for dealing with massive amounts of data and can be used to build powerful models for behavioural analysis (Abadi *et al*., 2016).

Hyperledger Fabric is a permissioned blockchain platform developed for enterprise applications that is used to implement the blockchain based audit mechanism. Hyperledger Fabric allows for the efficient and secure storage of records of transactions and support modular design, which makes it easier to integrate with cloud-based access control solutions. In this research, hyperledger fabric is employed to store the cryptographic hash of access logs to keep audit records immutable and intact without putting too much strain on the system (Androulaki *et al*., 2018).

The experimental environment is set up at a simulation server to emulate the behavior of a multi-tenant cloud system. The server is set to accept authentication requests, act like a user and make decisions on access in real-time. The simulation environment enables users to test various attack scenarios, such as credential misuse, abnormal access and cross-tenant access.

A processing pipeline for a dataset is implemented to process multiple datasets, which are used in this study. Data cleaning, feature extraction, normalization, and dataset merging are all included in the pipeline. The authentication logs from the LANL dataset are used for extracting user behaviour patterns and the network traffic features from the UNSW-NB15 and CICIDS2017 datasets are added to create network level anomalies. An integrated pipeline that takes into account both behavioral and network threats during evaluation.

Access scenarios are simulated by generating user sessions from historical patterns from the datasets to simulate realistic access scenarios. Both normal and malicious activities are included in the simulation. The malicious scenarios include things like unusual logon timings, device changes, fast logon attempts, and simulated cross-tenant logon requests. These scenarios are employed to test the capability of the framework of proposed anomaly detection and secure access policies.

The machine learning models are trained using supervised learning approach, and labeled data from the data sets are used to differentiate normal and anomalous behavior in the approach. The dataset is split in to training and testing sets, usually 80:20. The models are trained with the patterns of normal users' behavior, and during the test phase, the models are used to detect previously unseen anomalies. To ensure the model's accuracy and generalization, performance optimization methods like crossvalidation and hyperparameter tuning are implemented.

The machine learning models combined with the zero-trust policy engine provide dynamic access decision making. The machine learning model produces a behavioral risk score for every access request, which is then utilized with other context specific data, like user identity and device data. The system analyzes the security event according to pre-defined security thresholds, and decides whether the access is granted, denied, or if further security checks are required.

The framework has applied an off-chain/on-chain hybrid approach for integrating blockchain to make it perform efficiently. Access decisions are processed off-chain in real time to keep latency low while audit logs are hashes, and periodically uploaded to the blockchain. This design will ensure the system is maintained with high performance and also have secure and verifiable audit records (Casino *et al*., 2019) [6].

The experiments conducted in this study offer a complete setting to assess the developed SB-ZTAC framework in a realistic scenario. The configuration adopts a simulated multi-tenant cloud system with a combination of machine learning, zero trust principles, and blockchain-based auditing, thereby allowing comprehensive security effectiveness and system performance evaluation. The framework is assessed during its evaluation using classification performance measures (accuracy, precision, recall, and F1-score), system-level measures (inference latency, decision efficiency, and audit overhead).

7. Results and Evaluation

This section includes experimental results of the proposed Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC) on different datasets and machine learning models. Evaluation of the framework is done through the standard classification metrics including accuracy, precision, recall and f1-score, and system level metrics like inference latency and decision overhead.

The performance comparison of all the models evaluated in the three datasets (LANL, UNSW-NB15 and CICIDS2017) is summarized in Table 1.

Table 1: Performance comparison of machine learning models across LANL, UNSW-NB15, and CICIDS2017 datasets

Dataset	Model	Accuracy	Precision	Recall	F1 Score	Avg Latency (ms/sample)	Train Time (s)
LANL	Random Forest	0.9317	0.9472	0.9793	0.9630	0.0029	41.44
LANL	XGBoost	0.9309	0.9491	0.9762	0.9625	0.0027	6.13
LANL	Neural Network	0.9141	0.9290	0.9801	0.9539	—	—
UNSW	Random Forest	0.9398	0.9541	0.9516	0.9528	0.0056	27.40
UNSW	XGBoost	0.9434	0.9633	0.9476	0.9554	0.0052	8.35
UNSW	Neural Network	0.9189	0.9153	0.9620	0.9381	0.0723	12.01
CICIDS	Random Forest	0.9972	0.9970	0.9973	0.9972	0.0049	39.64
CICIDS	XGBoost	0.9990	0.9985	0.9995	0.9990	0.0028	7.79
CICIDS	Neural Network	0.9700	0.9549	0.9865	0.9705	0.0675	11.26

7.1 Machine Learning Model Performance

The results show that all three machine learning models, Random Forest, XGBoost, and Neural Networks, perform well on both datasets in detecting the anomalous access behavior. However, their performance varies depending on the characteristics of the data.

Both Random Forest and XGBoost show good performance on the LANL dataset, with an F1-scores of 0.963 and 0.962 respectively, which are large scale authentication logs. The model Neural Network has a slightly lower F1 score (0.954), but higher recall value, meaning it was able to identify a higher percentage of the anomalous activities. The results obtained demonstrate the high performance of ensemble based models with structured authentication data.

In the UNSW-NB15 dataset, XGBoost is the most effective model in terms of overall performance, with an F1 score of 0.955, surpassing Random Forest (0.953) and Neural Networks (0.938). Based on the results, it is concluded that the gradient boosting technique is very effective with complex network traffic features and also able to capture subtle patterns in the intrusion data.

All models have very high performance on the CICIDS2017 dataset with XGBoost getting the highest F1 score of 0.999. Random Forest has another remarkable F1 score of 0.997 and the Neural Network an F1 of 0.970. This near-perfect performance suggests that attack patterns in this dataset are highly distinguishable, though possibly less complex than real-world attack patterns.

The F1 score of each model on all datasets is shown in Fig 2, where one can see how well XGBoost performs on all datasets and that its performance is consistent across various data sources.

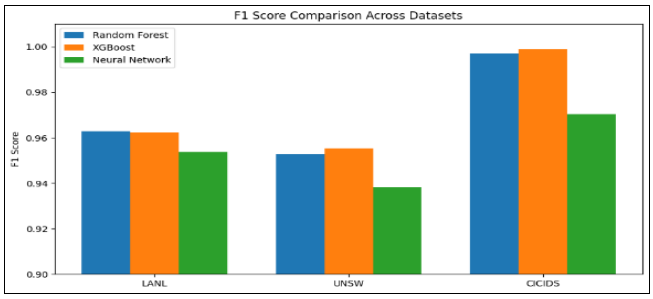

Fig 2: Comparison of F1-scores across LANL, UNSW-NB15, and CICIDS2017 datasets for Random Forest, XGBoost, and Neural Network models

7.2 Inference Latency and Efficiency

Besides the classification results, inference latency is also measured to ensure the appropriateness of the models in real-time access control systems. The results demonstrate that XGBoost has consistently the lowest latency across all datasets, as low as 0.0027 ms per sample on the LANL dataset and 0.0028 ms on the CICIDS dataset.

Random Forest has a slightly higher latency because of the ensemble nature and Neural Networks have a significantly higher latency especially on the UNSW and CICIDS datasets. This means that although Neural Networks provide robust detection, they are not necessarily best suited to latency sensitive applications.

The latency comparison is presented in Fig 3, which demonstrates that XGBoost offers the optimal performance/latency balance, making it ideal for real-time zero trust access control systems.

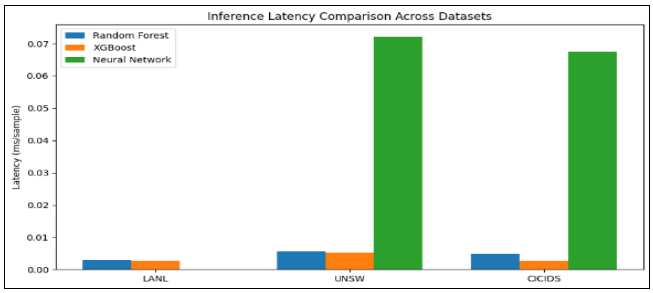

Fig 3: Inference latency comparison (ms per sample) of Random Forest, XGBoost, and Neural Network models across different datasets

7.3 Confusion Matrix Analysis

Confusion matrices of the best models for each dataset are further investigated to assess the classification performance. Random Forest model is selected as the best model for the LANL dataset, XGBoost model is selected for UNSW-NB15 dataset and the CICIDS2017 dataset.

As shown in Fig 4, the models' true positive rates are high and the false negative rates are relatively limited, which is essential for security applications. In the LANL dataset however, there are more false positives for legitimate access attempts, meaning that the legitimate access attempts are sometimes confused as anomalous. It underscores complexity of the behavioral authentication information and trade-offs of security sensitivity versus usability.

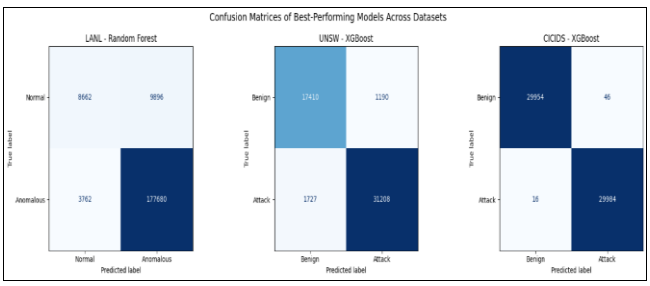

Fig 4: Confusion matrices of the best-performing models for each dataset: Random Forest for LANL, XGBoost for UNSW-NB15, and XGBoost for CICIDS2017

7.4 Zero-Trust Decision Evaluation

The threshold-based decision mechanism is used to test the effectiveness of the zero-trust part of the proposed framework by testing the model output. The attack block rate, legitimate access acceptance rate and false rejection rate are shown in Table 2 for each of the datasets.

The system has a high attack block rate (0.979) for the LANL dataset, but the legitimate access acceptance rate is relatively low (0.467) yielding a high number of false rejections. This means that in an authentication-based environment, access decisions might be conservative due to strict behaviour thresholds.

The UNSW-NB15 dataset, on the other hand, has a more even performance, with 0.962 being the attack block rate and 0.842 being the legitimate access acceptance rate. The dataset CICIDS2017 has excellent results when it comes to attack detection and very few false rejections, due to the separability of attack patterns in the dataset.

The results of a threshold sensitivity analysis also indicate that there exists a critical relationship between threshold sensitivity and trade-offs between security and usability. As shown in Table 3, lower thresholds (e.g., 0.3) yield higher attack detection rates, but also cause a higher number of false attacks to be rejected as nonattacks by legitimate users, which is especially problematic in the LANL dataset. On the other hand, higher thresholds (e.g., 0.7) increase the legitimate access acceptance rate, but decrease the detection capability of malicious activities.

The trade-off emphasizes the significance of adaptive threshold selection in zero-trust systems, a concept in which security policies need to be dynamically adjusted based on the operational environment to satisfy the usability requirements and strictness of access control.

Table 2: Zero-trust access control performance at threshold = 0.5 across different datasets

Dataset	Model	Threshold	Attack Block Rate	Legitimate Access Acceptance Rate	False Rejection Rate
LANL	Random Forest	0.5	0.9793	0.4668	0.5332
UNSW	Neural Network	0.5	0.9620	0.8425	0.1575
CICIDS	XGBoost	0.5	0.9995	0.9985	0.0015

Table 3: Impact of decision threshold on attack detection and access acceptance rates

Dataset	Model	Threshold	Attack Block Rate	Legitimate Access Acceptance Rate	False Rejection Rate
LANL	Random Forest	0.3	0.9988	0.1392	0.8608
LANL	Random Forest	0.5	0.9793	0.4668	0.5332
LANL	Random Forest	0.7	0.9121	0.9139	0.0861
UNSW	Neural Network	0.3	0.9977	0.7190	0.2810
UNSW	Neural Network	0.5	0.9620	0.8425	0.1575
UNSW	Neural Network	0.7	0.8769	0.9508	0.0492
CICIDS	XGBoost	0.3	0.9996	0.9975	0.0025
CICIDS	XGBoost	0.5	0.9995	0.9985	0.0015
CICIDS	XGBoost	0.7	0.9985	0.9990	0.0010

7.5 Blockchain-Based Audit Overhead

The auditing part of the blockchain is evaluated by simulating auditing logging latency and overhead. As illustrated in Table 4, the extra latency incurred by auditing is roughly 0.01 ms per event for all datasets.

The relative overhead percentage is large since the baseline decision latency is very low, but the absolute increase is small for real-time systems. For instance, the LANL dataset shows an increase in time per event from 0.000584 ms to 0.010783 ms, as shown in Table 4, which is still within the acceptable access control system range of high performance.

The results indicate that the adoption of blockchain auditing does not significantly affect system performance, and that blockchain technology offers robust assurances of data integrity and traceability. This shows that it is possible to implement secure, tamper-resistant logging systems into real-time zero-trust access control systems without a significant amount of latency.

Table 4: Performance overhead introduced by blockchain-based audit logging

Dataset	Model	Baseline Decision Latency (ms/event)	Decision + Audit Latency (ms/event)	Audit Overhead (ms/event)	Audit Overhead (%)
LANL	Random Forest	0.000584	0.010783	0.010199	1744.99
UNSW	Neural Network	0.000411	0.011092	0.010681	2596.58
CICIDS	XGBoost	0.000405	0.011193	0.010789	2666.98

8. Discussion

This research has shown that the use of behavioral analytics, combined with zero-trust access control and secure auditing systems can be effective in improving security in multi-tenant cloud environments. The results of the proposed SB-ZTAC framework demonstrate that the framework is effective on multiple data sets, supporting the success of integrating machine learning anomaly detection with dynamic access control policies.

The experimental results show that behavioral analysis is a significant factor in identifying abnormal usage patterns, especially when dealing with systems with high-volume authentication events and network traffic. Model results from the LANL dataset reveal that models like Random Forest and XGBoost have high recall, meaning that they are able to identify potential lateral movement and credential compromise. This is in line with previous studies by Ring *et al*. (2019) [19] that stress the significance of detecting abnormal user behavior and insider threats via authentication sequences analysis. Likewise, the machine learning effectiveness at intrusion detection in the UNSW and CICIDS datasets are similar to those reported by Buczak

and Guven (2016) [5] that data-driven models are capable of learning complex attack patterns in network environments.

One important finding is that model performance is highly sensitive to dataset characteristics. The ensemble models, especially XGBoost, generally show good performance in all the datasets, with the best accuracy and efficiency. This aligns with previous study conducted by Ahmad *et al*. (2021) [1] that Gradient Boosting techniques perform better than other models on structured Cybersecurity Dataset. Neural Networks, on the other hand, are more successful in several of the cases, making them appropriate for situations of higher risk where the ability to recognize all the possible attacks is more important than the number of false positives. Their increased latency, however, makes them less suitable to real-time access control systems, further demonstrating the tradeoff between accuracy and efficiency.

The analysis of the zero trust decision mechanism also indicates the real-life impact of integrating behavioral risk scoring into access control. Table 2 and Table 3 illustrate the impact of the threshold-based decision-making on security and usability. For instance, the LANL dataset has a high attack block rate with a relatively high false rejection rate; this means that the dataset is likely to be very conservative in making access decisions. This is in line with the basic tenets of Zero-Trust Architecture outlined by Rose *et al*. (2020) [20]: continual verification and the allowance for adaptive policy tuning without compromising usability. The threshold sensitivity analysis shows how the enforcement of the threshold can impact the number of false negatives and false positives in the real environment, underscoring the need for dynamic and context-aware policy enforcement in the real world.

One of the other key contributions of this study is the auditing study of blockchain to ensure secure access information logging. The results indicate that the added latency of audit logging is negligible when compared to the relatively large percentages. This indicates the possibility of embedding the immutable logging approach in real-time systems without negatively impacting performance. The results align with previous research conducted by Dorri *et al*. (2016) [9] and Zyskind *et al*. (2015) [29] that was able to show robust assurances of data integrity and tamper resistance while keeping system overhead reasonable. Additionally, by combining an off-chain/on-chain hybrid system, scalability is further improved and it is also in line with best practices that were identified in the latest blockchain security research.

Results also provide distinct information about the data sets. The near-perfect performance seen in the CICIDS2017 data set indicates the dataset might be less complicated than real-life enterprise environments as reported in other studies (Sharafaldin *et al*., 2018). The LANL set, by comparison, offers more realistic challenges – such as user behavior and noisy patterns of authentication – leading to higher false positive rates. This reiterates the need to assess security frameworks on a variety of data sets, so they can be generalizable and robust.

The proposed framework has performed well, but there are some issues to be noted. First, the blockchain-based auditing aspect is tested using a simulated audit logging latency and overhead instead of a real deployment of the auditing solution on a live blockchain network, which may limit the ability to assess real world scalability and transaction fees. Second, the zero-trust model is also applied by threshold-based decision rules; however, the complexity of adaptive policy engines that run in enterprise systems is not completely addressed. Third, however, while multiple datasets are employed, they might not adequately capture all kinds of real life cloud environments, especially highly dynamic and adversarial environments. Last, the models are trained with supervised learning, using data that are labeled, and may not be very good at generalizing to unseen patterns of attack.

9. Conclusion

This study aimed to overcome the limitations of traditional access control methods in multi-tenant cloud environments with a suggested Secure Behavioral Zero-Trust Access Control Framework (SB-ZTAC). The framework combines machine learning for behavioral anomaly detection, zero trust decision making, and blockchain for auditing to provide greater security, isolation, and accountability for tenants. The experimental validation with several cyber security datasets (LANL, UNSW-NB15 and CICIDS2017) shows the effectiveness of the proposed approach in detecting anomalous access patterns in various scenarios with high accuracy and F1-scores. XGBoost is one of the best models that are evaluated that offers a balance between performance in detecting the intruder and computational efficiency, suitable for real-time access control systems. The zero-trust evaluation also validates the importance of implementing threshold decision mechanisms to manage the security to usability trade-off while the audit simulation demonstrates that blockchain-based logging has near-zero latency penalty. Overall, the proposed SB-ZTAC framework is a scalable and practical solution for securing multi-tenant cloud systems. Further research is needed for practical deployment in cloud environments and integration with container systems, as well as creating adaptive policy engines for dynamic risk-aware access control.

10. Data Availability Statement

Data will be made available on request.

11. Funding

No funding.

12. Conflicts of Interest

The author(s) declare no conflicts of interest.

13. Ethical Approval and Consent to Participate

Not applicable.

14. References

1. Ahmad Z, Shahid Khan A, Wai Shiang C, Abdullah J, Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 2021; 32(1).
2. Ahmed M, Naser Mahmood A, Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016; 60:19-31.
3. Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem. Future Generation Computer Systems. 2016; 56:684-693.
4. Barka E, Sandhu R. A role-based delegation model and

some extensions. Proceedings of the 23rd National Information Systems Security Conference. 2000; 4:49-58.
5. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016; 18(2):1153-1176.
6. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics. 2019; 36:55-81.
7. Clarke EM, Grumberg O, Peled DA. Model Checking. Cambridge, Massachusetts, MIT Press, 1999.
8. De Moura L, Bjørner N. Z3: An efficient SMT solver. Lecture Notes in Computer Science, 2008, 337-340.
9. Dorri A, Kanhere S, Jurdak R. Blockchain in Internet of Things: Challenges and Solutions. IEEE Internet of Things Journal, 2016.
10. Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications. 2020; 50:102419.
11. Ferraiolo DF, Kuhn DR, Chandramouli R. Role-Based Access Control. 2nd edn. Boston, Artech House, 2007.
12. He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing. 2022; 1.
13. Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, *et al*. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Gaithersburg, National Institute of Standards and Technology, 2014.
14. Jin X, Krishnan R, Sandhu R. A unified attribute-based access control model covering DAC, MAC and RBAC. Lecture Notes in Computer Science, 2012, 41-55.
15. Kent AD. User-Computer Authentication Associations in Time. Los Alamos, Los Alamos National Laboratory, 2014.
16. Kent K, Souppaya MP. Guide to Computer Security Log Management. Gaithersburg, National Institute of Standards and Technology, 2006.
17. Kindervag J. Build Security into Your Network's DNA: The Zero Trust Network Architecture. Cambridge, Forrester Research, 2010.
18. Murata T. Petri nets: Properties, analysis, and applications. Proceedings of the IEEE. 1989; 77:541-580.
19. Ring M, Schlör D, Landes D, Hotho A. Flow-based network traffic generation using Generative Adversarial Networks. Computers & Security. 2019; 82:156-172.
20. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. Gaithersburg, National Institute of Standards and Technology, 2020. Report No: NIST SP 800-207.
21. Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. Computer. 1996; 29(2):38-47.
22. Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: A comparative review. Sustainability. 2022; 14(18):11213.
23. Servos D, Osborn SL. Current research and open problems in attribute-based access control. ACM Computing Surveys. 2017; 49(4):1-45.
24. Singer PW, Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, Oxford University Press, 2013.
25. Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection. 2010 IEEE Symposium on Security and Privacy, 2010, 305-316.
26. Waller A, Sandy I, Power E, Aivaloglou E, Skianis C, Muñoz A, *et al*. Policy based management for security in cloud computing. Communications in Computer and Information Science, 2011, 130-137.
27. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. Advances in Computers, 2018, 1-41.
28. Zhou M, Zhang R, Xie W, Qian W, Zhou A. Security and privacy in cloud computing: A survey. 2010 Sixth International Conference on Semantics, Knowledge and Grids, 2010, 105-112.
29. Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 2015, 180-184.