Journal of Intelligent Computing System (JICS), Vol.1, Issue. 3, pp. 93-105, (Sep 2026)
ISSN: 3139-3616 (online)

A Context-Aware Risk Scoring and Adaptive Access Control Model for Secure Web3 Applications

Prashant Soni[1], Yuvank Soni[2]
[1]Department of Computer Science and Engineering, Chandigarh University, Mohali, 140413, Punjab, India
[2]VP- Product Engineering, TAC Security, Mohali, 140307, Punjab, India
psoni.ps99@gmail.com, yuvanksoni@gmail.com

Abstract—Web3 applications provide decentralized and user-centric digital services through blockchain networks, smart contracts, and wallet-based identities. However, their dynamic transaction behavior, pseudonymous identities, and continuously changing access conditions introduce significant security challenges. Conventional access-control mechanisms primarily rely on static policies and predefined rules, limiting their ability to respond to evolving security risks. This paper proposes a context-aware risk scoring and adaptive access-control model for Web3 applications that integrates transaction context, wallet behavior, device/session information, and identity/credential status. These contextual features are normalized and combined using weighted risk scoring to classify access requests into low-risk, medium-risk, and high-risk levels. The proposed framework applies differentiated security actions, including normal authorization, step-up verification, and access denial, while continuously reassessing contextual changes. A reproducible simulation-based evaluation is conducted using legitimate, suspicious, and malicious access requests and compared with a rule-based baseline. On the held-out test set, the proposed model achieves 99.12% accuracy, 97.48% precision, 96.67% recall, and 97.07% F1-score, while maintaining a false-positive rate of 0.44%. The model also achieves an average decision latency of 12.66 ms, compared with 8.22 ms for the rule-based approach. Ablation analysis further demonstrates the contribution of the individual contextual feature categories to security performance. The results indicate that context-aware risk scoring can improve malicious-access detection and enable more granular adaptive security decisions for Web3 applications.

Index Terms—Web3 Security, Blockchain Security, Context-Aware Risk Scoring, Adaptive Access Control, Risk-Based Authentication, Wallet Behavior Analysis, Transaction Risk Assessment, Continuous Authentication, Anomaly Detection, Machine Learning, Smart Contracts, Decentralized Applications.

1. Introduction

The emergence of Web3 has brought about the rise of decentralized applications (DApps) which facilitate users to interact with blockchain networks utilizing identities based on wallets which are capable of executing smart contracts and exchanging digital assets. The Web3 ecosystem integrates decentralization, the blockchain technology, and intelligent technology in order to ensure greater control of users over digital assets and services [1]. At the same time, this decentralized approach poses certain security issues since users are expected to be responsible for authentication, transactions, and security measures to a lesser extent than before [2]. The introduction of decentralized identity management was developed with a view to giving users greater control over their digital identities and reducing their reliance on centralized identity stewards [3]. What is more, even though a successful identity verification does not necessarily imply that any transaction or access operation performed by that identity is trustworthy.

The use of blockchain technology for access control has been researched to see how effective it is in providing transparent and non-centralized authorization. Studies have indicated that both blockchain technologies and smart contracts can help in storing access control policies and executing them through operational execution without relying on central authorization stakeholders [4]. This has made access control more transparent and traceable, but traditional methods still lack efficiency when it comes to the changing risk connected to requests. Context-aware access control aims to overcome this by using information about the users, environment, behavior, and sensitivity of resources when making authorization decisions [5]. Using smart contracts in conjunction with context-aware methods proves that access control policies can be dynamically established based on changing contextual factors in decentralized environments [6].

Behavioral analysis adds a further dimension of security, as it allows for the tracking of how people use a certain system over time. Studies in behavioral authentication indicate that user behavior could be used for evaluating their action in terms of unexpected behavioral patterns to learn if there is something unusual happening in terms of continuous security assessment [7]. There are even privacy-preserving options

© 2026 JICS. Personal use is permitted, but republication/redistribution requires JICS permission.
see: https://synergyworldpress.com/journal/jics/about/overview

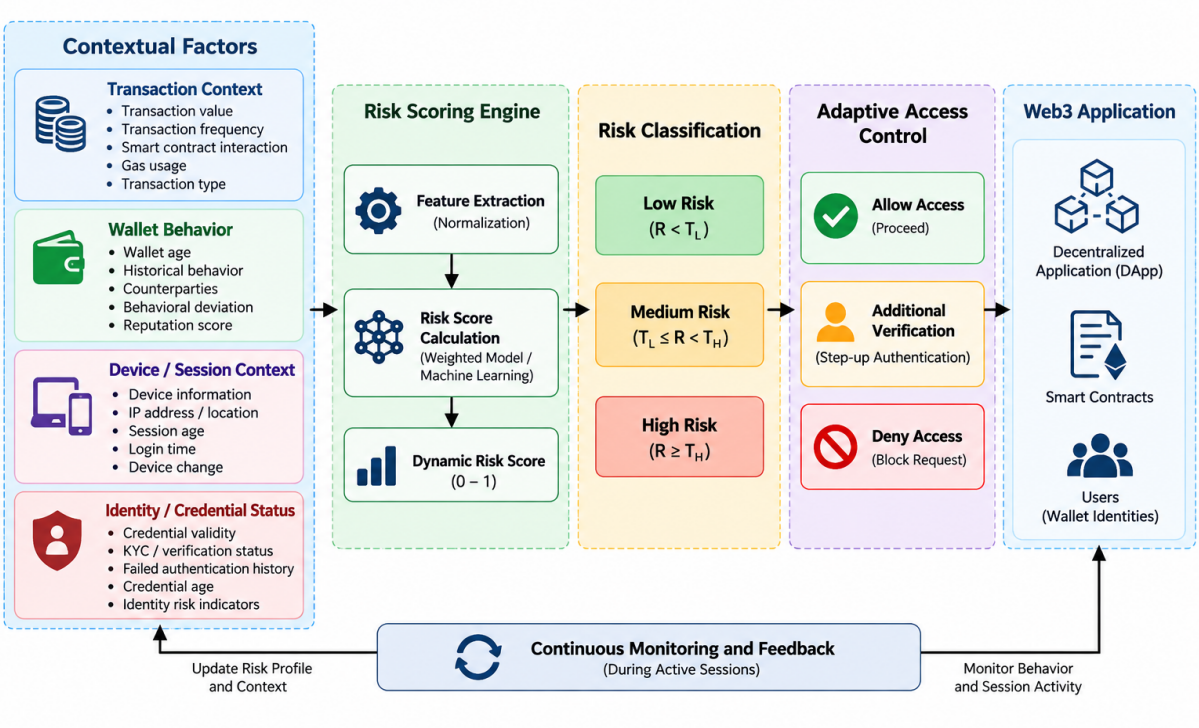


Figure 1. Overview of the proposed context-aware risk scoring and adaptive access control framework for Web3 applications.

of continuous authentication that allow one to monitor user behavior and thus check its legitimacy throughout a session without exposing behavioral info [8]. Analogous studies have demonstrated an ability of behavioral authentication to capture changes in user behavior in terms of his context and actions with the purpose of detecting any unauthorized actions [9]. Blockchain transactions are used to get useful information for recognizing suspicious actions since the transaction logs contain records about contracts, transfers, and wallet interactions. Research based on machine learning techniques has shown that fraudulent transactions in Ethereum can be recognized by using transaction-related attributes and classification methods [10]. Graph-based approaches offer more information by illustrating links between transactions and wallets, allowing for the identification of suspicious behavior patterns in addition to detecting any suspicious activity due to transaction characteristics [11]. Studies using temporal graph analysis suggest that the timing of transactions impacts the detection of scams [12]. More from recent research is the integration of transaction semantics with graph representation learning approaches to study the features of transactions and the relations between accounts on blockchain [13].

While these methods offer good ways to spot questionable behavior in blockchain systems, detecting threats and controlling access are normally viewed as independent operations. Research into blockchain access control that takes risks into account has shown that it is possible to combine historical behavior with information about the current situation, which can be used for drawing flexible authorization decisions [14]. Modern adaptive architectures have also proved to be capable of combining different authentication and access control methods with risk assessment based on artificial intelligence for employing a variety of response mechanisms such as approval, re-authentication, blocking, etc. instead of relying on fixed authorization procedures [15].

Even though there have been advancements in Web3 behavioral and transaction analysis as well as adaptive access control, a gap still exists. Existing studies generally deal with various security functions like decentralized identity, blockchain authorization, behavioral authentication, fraud detection, and anomaly detection. However, not much literature exists for a combined system that allows transaction context, wallet behavior, device/session context, and credentials status to be combined into a dynamic risk score, and then be used to produce an adaptive authorization decision. This paper proposes a model of context-based risk scoring and adaptive access control in order to fill this gap. The proposed model classifies requests into low-risk, medium-risk, and high-risk. Low-risk requests are allowed, medium-risk requests are verified further, and high-risk ones are rejected as shown in Fig. 1. The main contributions of the proposed model concern contextual risk assessment, dynamic risk scoring, adaptive access control, continuous session monitoring, and evaluation through attack detection, false-positive rate, classification performance, and decision latency.

2. Literature Review

The upsurge in the popularity of various blockchain platforms and decentralized applications has created an interest in several areas of study such as secure identity management, access control, behavior analysis, and intelligent threat detection. Earlier studies have made use of blockchain-based authorization, contextual risk assessment, machine learning, graph analysis, and adaptive authentication technologies to investigate these topics. However, the research conducted in these areas have either been carried out separately or independently. The literature in the field of blockchain access control, context-aware risk assessment, Web3 behavior analysis, and adaptive authentication has been reviewed to ensure that the intention of the proposed model is fulfilled.

2.1 Blockchain-Based Access Control and Decentralized Identity

Blockchain technology has been increasingly studied as a method for decentralized access control due to its inherent ability to enable authorization processes which are auditable and do not completely rely on a central authority. Wu et al. [16] proposed an access-control system based on the use of blockchain to protect confidential attributes and access policies by allowing fine-grained authorization. Their experiments with Hyperledger Fabric showed that blockchain can be efficient in giving decentralized enforcement of policies; however, the method is still very much focused on policies and attributes and does not take risks into account dynamically. Singh et al. [17] presented a review of blockchain-based access-control techniques to thwart cyber attacks, highlighting the application of smart contracts for decentralized management of the policies. Such study has also determined the main advantages of blockchain access control, including decentralization, transparency, auditability, and immutability, as well as emphasized some challenges of using blockchain regarding scalability, privacy, and dynamic authorization. Moreover, a similar research was made by Bagga et al. [18], who surveyed access-control techniques based on blockchain and emphasized the shift from old-style centralized authorization to decentralized approaches. Thus, these studies show that blockchain serves as a great basis for the storage and verification of access policy. Decentralized identity has opened up another essential component of access management in Web3. Yan et al. [19] studied decentralized identity management in detail and reviewed142 articles on identity tasks and stakeholders, self-sovereign identity as well as interoperability. As a result, their research concluded that decentralized identity will ensure user empowerment and identity value management but will also pose certain issues of interoperability, governance and implementation. An approach founded on decentralized identity and access control and interpreted as blockchain-aware by other researchers has demonstrated that it is indeed possible to prove the authenticity of self-sovereign identities without the need of relying on a centralized authorizing party [20]. Bringing such techniques into use makes it possible to have reliable identity information; however, identity authentication does not mean that every operation performed by an identity can be trusted.

2.2 Context-Aware and Risk-Based Access Control

Standard methods of authorization typically rely on a fixed set of permissions and stable characteristics of users. Context-aware approaches aim to deal with this limitation by introducing some external elements involved in describing the environment, behaviors of users, the degree of sensitivity of the resources and other access conditions applicable at the moment. The authors [21] developed a model of context-aware attribute-based access control that includes user identity, environmental data, behavioral data, the level of resource and activity sensitivity as well as the risk history. The model assesses the risk of access request and compares its result with the already established risk policies. They also introduced a combined weighting process based on game theory. In the same study, it was shown that risk-aware authorization could achieve finer-grained decisions compared to traditional attribute-based access control (ABAC). The prototype of this system has analyzed 100 users and compared the expense of decision-making in context-aware and risk-based systems versus ABAC, concluding that the total risk assessment costs were relatively low. Nevertheless, it was designed as a general framework rather than a system for Web3 transactions, wallets' usage, and decentralized identities.

MRAAC was proposed by Chen et al. [22], standing for multi-stage risk-aware adaptive authentication and access control. It changes its authentication requirement based on contextual, behavioral information, resources' sensitivity, and authenticity of the user. This multi-stage approach clearly demonstrates that the process of authorization could go hand in hand with different types of authentication instead of a binary decision. Another similar project was developed by Merlec [23]; their SC-CAAC is a context-aware access control system based on smart contracts designed for IoT systems based on blockchain.

2.3 Behavioral and Machine-Learning-Based Web3 Security

The data available within transaction records make machine learning an effective method for recognizing irregular blockchain transactions because those records contain behavior data suitable for analysis. Research

conducted by Onu et al. [24] comprised various models including random forests, neural networks, and K-nearest neighbor in conformity with analyzing more than 20,000 transactions associated with Ethereum Ponzi schemes. The researchers reached the conclusion that machine learning enables the identification of fraudulent transactions involving Ethereum, but they should note that the research was aimed at detecting one kind of fraud and not the general one.

Similarly, research work conducted by Xiong et al. [25] used graph neural networks for stealing identification, with the help of the process called TransWalk that incorporates transaction network random walks and multi-scale feature extraction for detecting fraudulent activities involving Ethereum. Recent studies in this area led to new findings. For instance, Sun et al. [26] suggested an Ethereum fraud detection method that merges transaction language modeling and graph representation learning. This method is capable of identifying transaction semantics as well as relation of accounts, thus overcoming the drawbacks of the methods that utilize only sequence or graph information. Another semi-supervised method, Cluster-GAT, further develops Ethereum fraud detection techniques by dividing the huge transaction graph into smaller ones and utilizing GNNs given lack of labeled information on fraud data [27].

Moreover, other research in the area of anomaly detection in blockchain indicates that machine learning solutions are moving beyond the principle of fixed rules. Thus, Cholevas et al. [28] reviewed the according methods of unsupervised anomaly detection in blockchain networks and underlined the importance of identifying deviations from the normal behavior. Another study has shown the usefulness of combining machine learning classifiers with explainability methods for the purposes of anomaly detection [29].

2.4 Adaptive Authentication and Continuous Security

Continuous authentication provides supplementary security strategies by consistently examining if the individual user or the ongoing session is trustworthy. Baig et al. [30] evaluated privacy-preserving continuous authentication based on behavioral biometrics, proving the use of behavioral and situational information through authentication processes across the duration of one session instead only on initial logging in. The research also illustrated issues of privacy in connection with constant behavioral information collection. Research in behavioral authentication also emphasizes that safety decisions can be made based on whether a certain action is suited to an individual user's situation.

The research on adaptive access control reinforces the link between real-time trust assessment and the adaptation of applicable policies. The risk-adaptive access control model applied to service meshes relies on a behavioral trust evaluation technique that helps define whether the access policy needs to change in case of a trust-level shift regarding the requesting service. Besides, blockchain-related risk-adaptive models demonstrated the possibility of changing access or data-sharing policies dynamically based on risk assessment rather than using conventional binary decisions.

2.5 Research Gap

The reviewed studies indicate that blockchain-based access control, context-aware risk assessment, machine-learning-based threat detection, and adaptive authentication have developed as important but largely separate research directions. Existing blockchain access-control approaches primarily focus on decentralized and auditable authorization, while context-aware methods emphasize dynamic evaluation of access conditions. Similarly, Web3 security approaches mainly analyze transaction and wallet behavior to identify suspicious activities, whereas adaptive authentication methods focus on changing security requirements according to evolving user and session conditions. Despite these developments, a unified approach that connects these security functions within a single Web3 access-control process remains limited. Existing methods generally do not simultaneously consider transaction characteristics, wallet behavior, device and session context, and credential status when making an access decision. This motivates the proposed model, which integrates these contextual factors into a dynamic risk assessment mechanism and converts the resulting risk level into an appropriate security response. The objective is to provide a more flexible and context-sensitive access-control mechanism capable of adapting to changing security conditions in Web3 applications.

3. Proposed Methodology

This section presents the proposed context-specific risk scoring and adaptive access-control model for secure Web3 applications. This framework brings together the collection of contextual information, risk score calculation, risk classification, adaptive authorization, and permanent session supervision. The proposed model assesses the security environment for any request or transaction made on the blockchain and assigns a risk score. The risk level is then used to decide on providing access to the request. The scheme of the approach can be seen in Fig. 2.

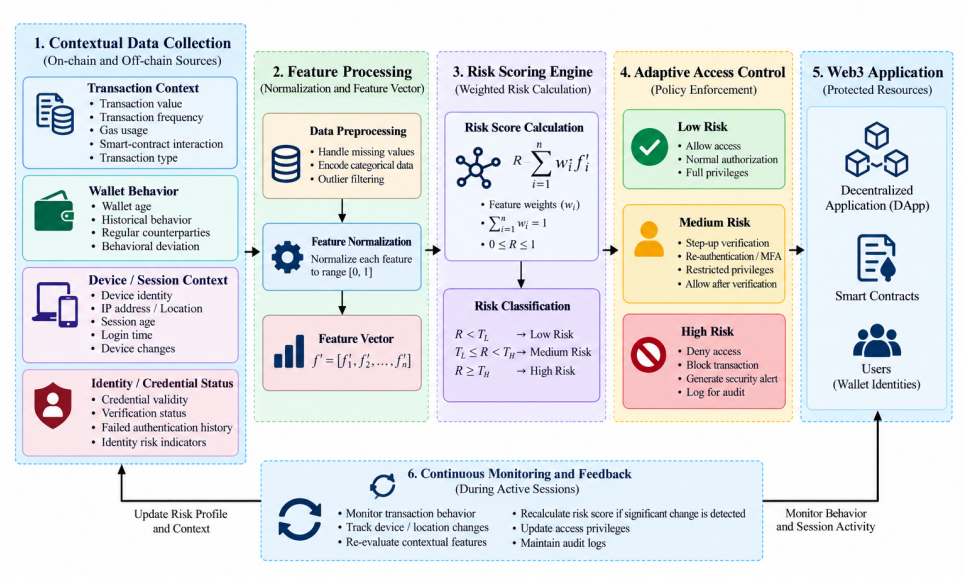


Figure 2. Proposed methodology for context-aware risk scoring and adaptive access control in Web3 applications.

3.1 System Overview

The suggested framework works through a total of five phases. These phases include the gathering of contextual data, processing of features, assessment of risks, adaptive access control, and constant monitoring. If an access request is sent, the framework gathers details connected to the transaction, wallet behavior, device/session status, and identity/credential status. The gathered data is normalized and sent to the risk-scoring engine.

Afterward, the risk-scoring engine generates a risk score from 0 to 1. This value is than checked against two preset thresholds that are designed to categorize the request as low, medium, or high risk. A low-risk request is granted access, a medium-risk request goes through an additional verification process, and a high-risk request is denied access. Making a decision does not involve only the first request but also continuous monitoring of the active sessions in order to recalculate the risk score after critical changes in context.

3.2 Contextual Feature Model

For risk assessment, there are four different contextual categories namely transaction context, wallet behavior, device/session context, and identity/credential status. The transaction context considers parameters like transaction value, transaction frequency, usage of gas, and interaction with smart contracts. On the other hand, wallet behavior is about the age of the wallet, past transaction behavior, counter parties involved on a regular basis, and the variance from the normal behavioral pattern. The device/session context states the device identity, information about the location or IP address, the age of the session, time of login, and number of times device has been changed. The last contextual category of identity and credential status deals with credentials that are valid, verification status, and failure of previous authentications.

Table I. Contextual Features Used for Risk Assessment

Feature Category	Example Features
Transaction Context	Transaction value, transaction frequency, gas usage, smart-contract interaction
Wallet Behavior	Wallet age, historical transaction behavior, regular counterparties, behavioral deviation
Device/Session Context	Device identity, IP/location, session age, login time, device changes
Identity/Credential Status	Credential validity, verification status, previous authentication failures

In order to select features, both current access requests and historical behavior of requestors are considered. Current transactions and device information represent the immediate access context, but wallet and authentication history represents a previous behavior.This combination enables the framework to evaluate the current security context together with historical patterns for risk assessment, as presented in Table I.

3.3 Risk Score Calculation

Before risk calculation, each contextual feature is normalized to a common range from 0 to 1. For a feature f_i, the normalized value is represented as f_i', where higher values indicate greater security risk. The overall risk score is calculated as

$$R = \sum_{i=1}^{n} w_i f_i' \tag{1}$$

where R represents the overall risk score, w_i is the weight assigned to the i-th feature, f_i' is its normalized value, and n is the total number of contextual features. The weights satisfy

$$\sum_{i=1}^{n} w_i = 1 \tag{2}$$

so that the resulting risk score remains within the range $0 \leq R \leq 1$.

The feature weights are determined during the model-development stage using the validation data and are then fixed before testing. This prevents the test data from influencing the risk calculation. The relative contribution of each contextual factor therefore remains unchanged during evaluation.

Two decision thresholds, T_L and T_H, are used to convert the continuous risk score into a security level:

$$R < T_L \Rightarrow \text{Low Risk} \tag{3}$$

$$T_L \leq R < T_H \Rightarrow \text{Medium Risk} \tag{4}$$

$$R \geq T_H \Rightarrow \text{High Risk} \tag{5}$$

The thresholds are selected using the validation set by considering the trade-off between detecting malicious requests and avoiding unnecessary restrictions on legitimate users. Once selected, the thresholds remain fixed during testing.

3.4 Adaptive Access Decision

The authorization action employed for an access request is determined by the risk level associated with it. Low-risk requests are allowed through the standard authorization process as the observed contextual parameters match expected behavior. Medium-risk requests, on the other hand, will not be rejected immediately; instead, they will involve step-up verification such as re-authentication or further identity verification prior to completing the operation. High-risk requests will be denied and may generate a security alert or audit event. The adaptive mechanism can also change the active session's prevailing privilege. A session rated as low risk may gain a stricter security status due to the increased risk score generated through some strange transaction, device alteration, behavioral variation, repetitive authentication failure, or any other contextual change. Likewise, a request rated as medium risk can go back to the standard authorization status once any verification is completed successfully, and the contextual parameters are found acceptable. Therefore, authorization is considered a dynamic process instead of a one-time action that is essential only at the moment of login.

3.5 Continuous Monitoring

After the access decision has been made, the framework will track necessary transactional, wallet, device, and credential parameters during the entire session. New contextual data will be matched with the existing security profile. If all the conditions are within the established limits, the corresponding authorization status is maintained. However, if a significant contextual variation occurs, the corresponding elements are updated and the risk score is calculated anew. The new score is calculated and compared with the previously set limits which leads to the application of the corresponding access model. Moving from low to medium risk requires additional verification, while transition to a high-risk category means denial of the operation. The use of the continuous feedback mechanism allows the system to react to security changes during the session rather than only relying on the results of initial authentication.

4. Experimental Setup

The experimental design has been devised to verify the proposed context-dependent scoring of risk and adaptive model control in normal, suspicious, and threatening Web3 access. The evaluation checks how well the proposed model can identify risky actions, respond accordingly using security measures, and ensure low decision overhead. Conventional rule-based access control is adopted as the main baseline for the experiment comparison.

4.1 Experimental Environment

The framework presented here is estimated in the Web3 application environment that features a blockchain layer, wallet-based user interaction, contextual data collection, risk scoring, and adaptive access-control blocks. A request for access includes information on transactions, wallets, devices, sessions, and identities. The proposed system processes mentioned features and derives a normalized risk score and corresponding risk class. At the end of the experiment, it is presented the whole implementation capturing input context, risk score obtained, risk classification results, the action taken, and decision delay of a concrete request.

4.2 Access Scenario Configuration

The three types of access requests include legitimate access requests, suspicious access requests, and malicious access requests. Legitimate access requests are those that conform to the normal wallet behavior or transaction behavior. Suspicious access requests are characterized by unusual transaction values or levels of transaction activity, attempts to use unknown devices or locations, and changes in previous wallet behavior. The malicious access requests are deceptive access attempts meant to execute unauthorized access requests. Each of these scenarios is considered both in the proposed approach and in the baseline in order to make a comparison of the two methods.

Table II. Experimental Configuration

Parameter	**Configuration**
Application Environment	Web3 decentralized application
Blockchain Layer	Ethereum-compatible network
User Interaction	Wallet-based access
Context Categories	Transaction, Wallet, Device/Session, Identity/Credential
Risk Score Range	0–1
Risk Levels	Low, Medium, High
Low-Risk Action	Allow access
Medium-Risk Action	Step-up verification
High-Risk Action	Deny access / security alert
Baseline	Rule-based access control
Evaluation	Legitimate, suspicious, and malicious requests
Metrics	Accuracy, Precision, Recall, F1-score, FPR, Latency, Computational Overhead

The proposed method uses three levels of risk classification specifically developed for access requests so that each request is classified into low risk, medium risk, or high risk requests. Low risk requests are approved, medium risk requests are checked while high risk requests are rejected. Changes in the context of the active sessions can lead to a re-evaluation of the access requests and a change in the access method. The test scenarios and context features used in the evaluation are presented in Table I.

4.3 Performance Evaluation Metrics

The efficacy of the proposed model is evaluated using parameters such as accuracy in terms of attack detection, precision, recall, F1-score, false-positive rate, response time and computation overhead. Accuracy represents the percentage of requests correctly classified, while precision and recall signify the dependability and comprehensiveness of detection of malicious requests respectively. The F1-score is a summary metric that takes into account both precision and recall.

The F1-score is calculated as

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{6}$$

The false-positive rate is calculated as

$$FPR = \frac{FP}{FP + TN} \times 100 \tag{7}$$

where FP represents legitimate requests incorrectly classified as risky and TN represents legitimate requests correctly classified as safe.

The measurement of decision latency runs from when the access request is received to when the final decision is made. The measurement of computational overhead runs from the extra processing needed to determine the various contextual features and calculate a risk score. The two important metrics are used to understand whether the addition of security assessment will yield more protection while still keeping the decision costs manageable.

4.4 Comparative and Ablation Evaluation

In this study, the new approach is compared to the existing rule-based technique while using the same access scenarios and context inputs. The model is subjected to an ablation study by taking out main context categories and testing their relevance in the final performance of the approach. The configurations used include instances without transaction context, wallet behavior, device/session context, and identity/credential status.

The study also includes threshold sensitivity testing performed by changing low-risk and high-risk thresholds during the validation stage and checking the impact of thresholds on detection accuracy, false-positive rate, and decision latency of the detection events. Finally, the thresholds used during the evaluation phase are settled to avoid test time leakage.

5. Results and Performance Evaluation

The proposed context-aware risk scoring and adaptive access-control model was evaluated to assess its contribution to enhancing the security of Web3 applications. This evaluation is based on five important factors: detection of attacks, classification of risk, false-positive rate, decision latency, and improved security. The above parameters provide a good impression of the model's capabilities in terms of detecting unwanted actions, differentiating between different levels of risk, making access decisions at the right time, and preventing unnecessary restrictions on bona fide users. In addition, the proposed method is compared with a conventional rule-based approach to assess the benefits of incorporating context-based assessment into the decision-making process. Moreover, the impact of additional risk assessment on security enhancement is examined while maintaining decision-making performance appropriate for the dynamic nature of Web3 applications.

5.1 Attack Detection Analysis

The detection performance of the proposed model was assessed on the held-out test requests and contrasted against the performance of the rule-based method. The assessment included accuracy, precision, recall, F1-score, and false positive rate. According to the data provided in Fig 3, the proposed model performed better overall but had a specially good ability of identifying harmful requests. Recall and F1-score were higher than those of rule-based method, which shows that the model was more effective in identifying harmful actions than the rule-based method.

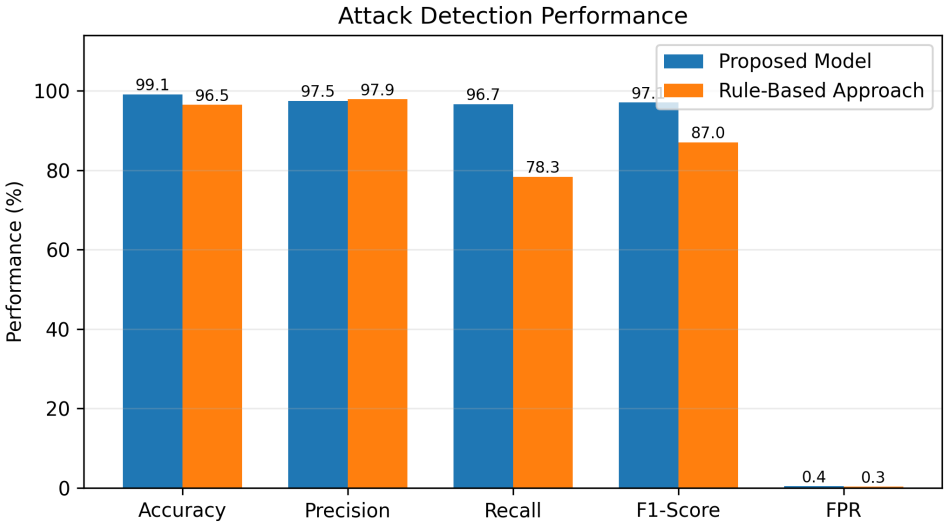


Figure 3. Attack detection performance comparison between the proposed model and the rule-based approach.

The alternative system also improves the detection of suspicious requests which could otherwise look like everyday user behavior. Looking at all relevant contextual signals at the same time, the system can detect

strange transaction patterns, unusual wallet activity, changes in device and session usage, and authentication-related anomalies, which might be missed by single rule-based analysis. The use of multiple factors ensures a more reliable attack detection and better-informed decisions in terms of protection strategies to use for Web3 access requests.

5.2 Risk Classification Analysis

The ability of the proposed model to classify access requests into low-risk, medium-risk, and high-risk categories was evaluated using the held-out test set. The classification was performed using the risk thresholds selected during the validation stage, with $T_L = 0.32$ and $T_H = 0.56$. The categorization of requests into risk levels was done based on their aggregated context-based risk scores. As observed in Fig. 4, the majority of legitimate requests have been placed into the low-risk category, while suspicious requests have been assigned to the medium-risk category more often than to others. The malicious requests show a much higher ratio of their placement in the high-risk category which indicates that the system used hints at how different contextual features may be used for the separation of requests in terms of access. The fact that medium-risk has been introduced is of special significance because it helps suspicious requests to be verified in a proper way instead of getting accepted or rejected immediately. Thus, the three-level classification of requests allows the implementation of differentiated security measures based on the risk associated with each request. The classification demonstrates the efficiency of the risk assessment mechanism implemented as a part of the access control process in Web3.

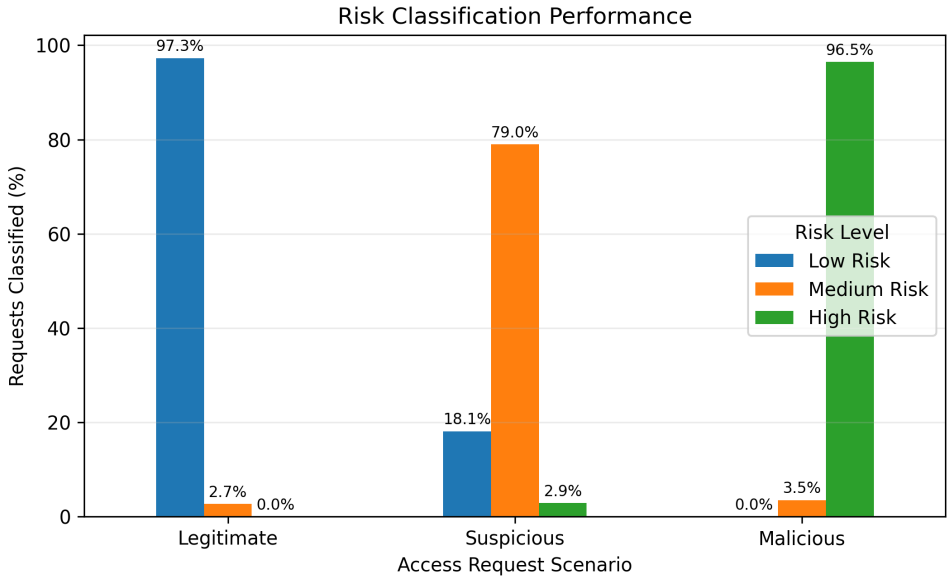


Figure 4. Risk classification performance for low-risk, medium-risk, and high-risk Web3 access requests.

5.3 False-Positive Rate Analysis

The false-positive rate (FPR) was found in order to measure the efficacy of the tested algorithm in mislabeling legitimate requests to gain access as malevolent. The FPR was measured over the dataset that had not previously been used for training, and was based on the number of legitimate requests misclassified as well as the total number of legitimate requests. The FPR is defined as:

$$FPR = \frac{FP}{FP + TN} \times 100 \tag{8}$$

where FP represents legitimate requests incorrectly classified as malicious and TN represents legitimate requests correctly accepted as non-malicious. As shown in Fig. 5, the proposed model achieved an FPR of 0.44%, compared with 0.29% for the rule-based approach. Although the rule-based approach produced a slightly lower FPR, the proposed model provided substantially higher recall and F1-score for malicious-request detection. This indicates that there is a slight increase in the number of false positives, while the efficiency in detecting malevolent attempts is very high. As a result, there is an evident trade-off between the varying degrees of restriciveness of the access that is being granted and the efficiency of the security measures taken.

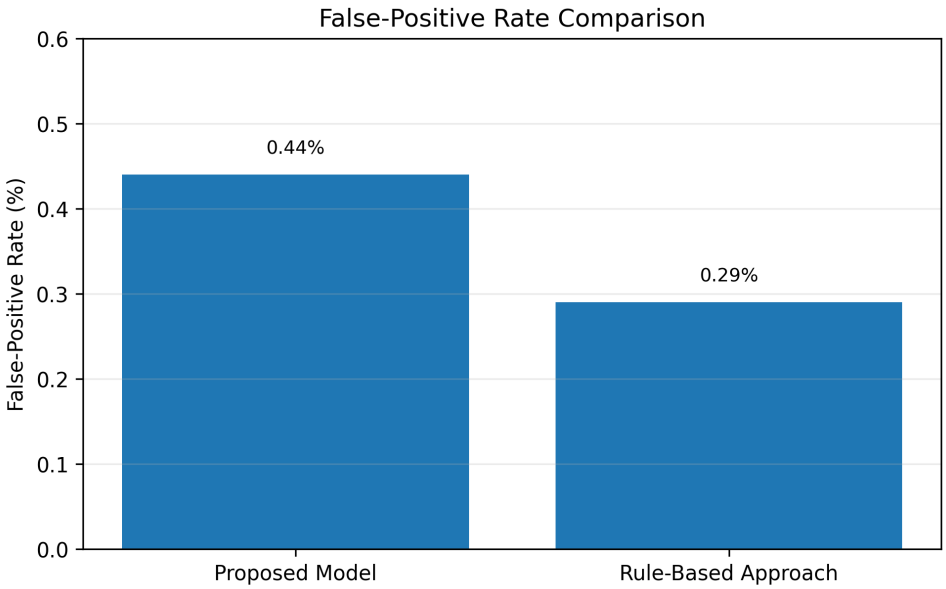


Figure 5. False-positive rate comparison between the proposed model and the rule-based approach.

5.4 Decision Latency Analysis

The latency of decisions was measured to determine the interval between the submission of the access request and the formulation of final authorization. Such latency includes the time needed for processing the contextual features, computing the risk score, assigning a risk level stress, and applying the access-control policy in accordance with this.

The compared model has used a rule-based approach in the same assignment. Such a comparison deserves a lot of attention as these adaptive mechanisms might work efficiently when applied in situations, which involve detection. At the same time, a practical Web3 mechanism should allow establishing an optimal latency for taking any decisions concerning access to the resource.

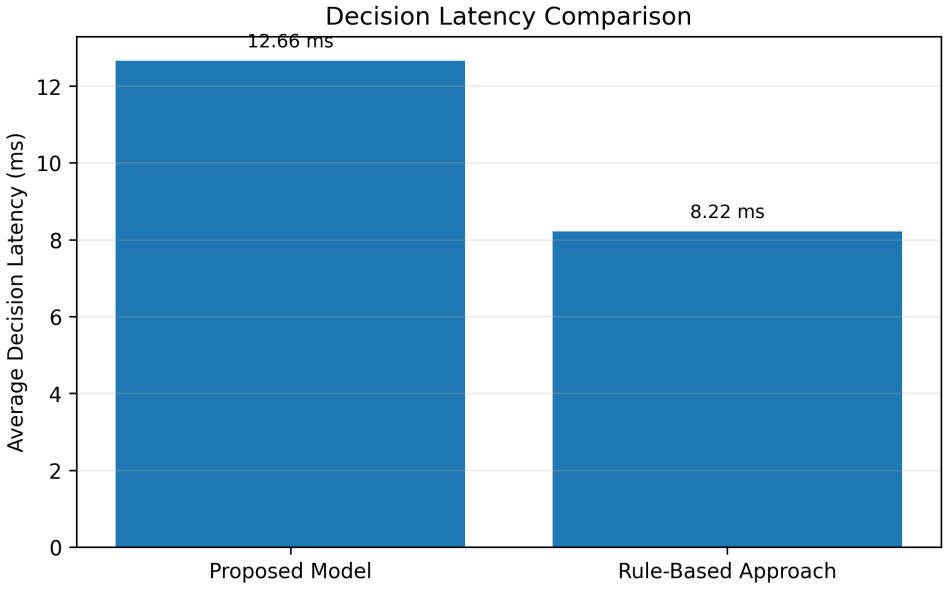


Figure 6. Average access decision latency of the proposed model and the rule-based approach.

The author has calculated the decision latency upon the arrival of the request to the access-control layer and till the moment it has formulated a decision about the authorization. The average latency calculated from the experimental test run results is provided in Fig. 6. The approach suggested necessitates extra processing as it assesses many contextual factors before making an access decision. Nevertheless, this extra processing allows the system to differentiate various risk situations and act accordingly to the current situation like normal access,

step-up authentication, or access denial. As a result, the latency results become an important indicator of the computing feasibility of the proposed adaptive access control method for Web3 applications.

5.5 Security Improvement Analysis

The overall security improvement of the proposed framework was evaluated by comparing its detection performance with the rule-based access-control approach on the held-out test set. The evaluation considers accuracy, precision, recall, F1-score, and false-positive rate to determine whether contextual risk scoring provides a more effective security decision mechanism.

The proposed model achieved an accuracy of 99.12%, compared with 96.50% for the rule-based approach. Its recall also increased substantially from 78.33% to 96.67%, indicating that the proposed framework was able to identify a considerably larger proportion of malicious access requests. Similarly, the F1-score improved from 87.04% for the baseline to 97.07% for the proposed model, demonstrating a better balance between malicious-request detection and precision.

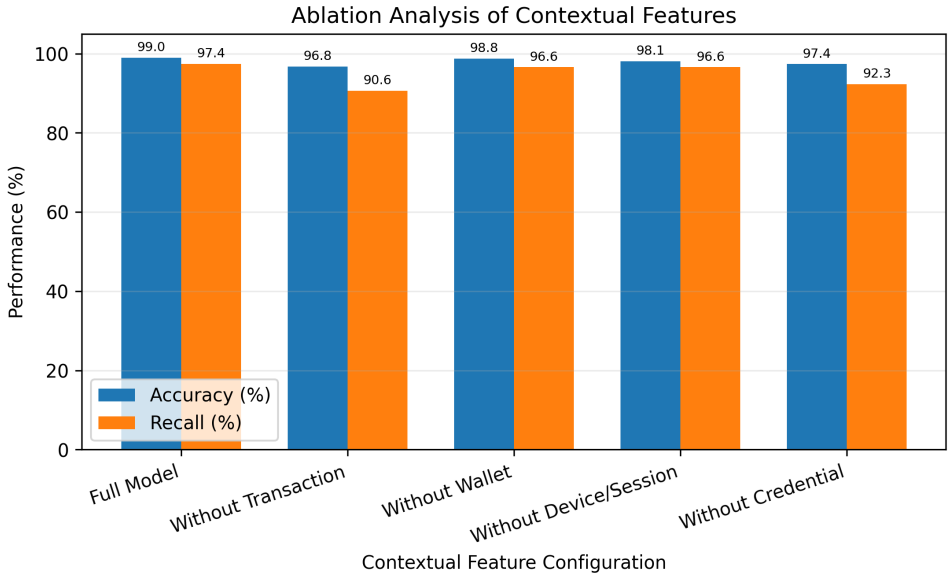


Figure 7. Overall security improvement of the proposed context-aware adaptive access-control model.

Although the rule-based approach produced a slightly lower false-positive rate of 0.29%, the proposed model maintained a low FPR of 0.44% while providing considerably higher recall and F1-score.The trade-off shows that using context in a model enhances security efficiency without causing many incorrect malicious classifications to happen. Findings indicate that the mix of contextual data such as transacting, wallet-related details, devices, and accounts leads to better access control rules in comparison to using only predetermined rules.

Summing up, comparison results illustrate that the suggested framework allows for better malicious request detection as well as risk-based decision making while keeping to a low level of false positives. Findings show that adaptive risk scoring can be an important safeguard for Web3 applications due to possible changes in the user context and conditions.

6. Conclusion and Future Work

A context-aware risk scoring and adaptive access control framework that protects Web3 applications from dynamic and harmful access conditions was introduced. The method takes into account the transaction context, wallet behavior, device and session information, and identity and credentials to create a risk score normalized in the range between 0 and 1. Based on the defined thresholds being determined by the validation, access requests can be classified into three groups, namely low-risk, medium-risk, and high-risk ones, which allows for different security measures being taken. The evaluation using the held-out test set demonstrated that the proposed approach achieved 99.12

The risk-classification analysis further showed that 97.29% of legitimate requests were classified as low risk, while 79.00% of suspicious requests were classified as medium risk and 96.50% of malicious requests were classified as high risk. The decision-latency evaluation showed an average latency of 12.66 ms for the proposed model compared with 8.22 ms for the rule-based approach. Although contextual evaluation

introduces additional processing overhead, the measured latency remained in the millisecond range. The ablation analysis also demonstrated that removing contextual categories reduced detection performance, particularly when transaction or credential information was excluded. These findings support the effectiveness of combining multiple contextual signals for adaptive Web3 access control.

Future work will focus on validating the proposed framework using real-world Web3 transaction and access-control datasets and deployment within operational decentralized applications. Additional research is required to evaluate the model under different blockchain networks, wallet behaviors, transaction patterns, and application architectures.

The risk-scoring mechanism can also be extended with additional contextual signals, including smart-contract reputation, historical attack indicators, cross-wallet relationships, and temporal behavioral patterns. Machine-learning and graph-based models may be investigated to automatically learn complex relationships among these features while maintaining interpretable risk decisions.

Another important direction is the evaluation of adversarial attacks against the risk-scoring mechanism, particularly context manipulation, device or location spoofing, and attempts to gradually establish trusted behavior before requesting elevated privileges. Future experiments will investigate the robustness of the framework against such attacks and evaluate mechanisms for detecting manipulated contextual information.

References

[1] J. Zhu, F. Li, and J. Chen, "A survey of blockchain, artificial intelligence, and edge computing for Web 3.0," *Computer Science Review*, vol. 54, Art. no. 100667, Nov. 2024, doi: 10.1016/j.cosrev.2024.100667.

[2] J. J. Si, T. Sharma, and K. Y. Wang, "Understanding User-Perceived Security Risks and Mitigation Strategies in the Web3 Ecosystem," in *Proc. CHI Conf. Human Factors in Computing Systems (CHI '24)*, 2024, Art. no. 974, pp. 1–22, doi: 10.1145/3613904.3642291.

[3] F. Schardong and R. Custódio, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," *Sensors*, vol. 22, no. 15, Art. no. 5641, 2022, doi: 10.3390/s22155641.

[4] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, Art. no. 146, 2024, doi: 10.1186/s13677-024-00697-7.

[5] R. Shevchuk, B. Adamyk, V. Benson, O. Kovalchuk, M. Bernas, and V. Martsenyuk, "CAHE-AML: Context-Aware Hybrid Encryption Framework for Secure Cross-Border AML Data Sharing in Cryptocurrency Ecosystems," *Electronics*, vol. 15, Art. no. 3202, 2026, doi: 10.3390/electronics15143202.

[6] C. Cheng, B. Yan, and G. Wang, "The blockchain based access control scheme for the Internet of Things," *Procedia Computer Science*, vol. 202, pp. 342–347, 2022, doi: 10.1016/j.procs.2022.04.046.

[7] C. Wang, H. Tang, H. Zhu, J. Zheng, and C. Jiang, "Behavioral authentication for security and safety," *Security and Safety*, vol. 3, Art. no. 2024003, 2024, doi: 10.1051/sands/2024003.

[8] A. F. Baig, S. Eskeland, and B. Yang, "Privacy-preserving continuous authentication using behavioral biometrics," *International Journal of Information Security*, vol. 22, pp. 1833–1847, 2023, doi: 10.1007/s10207-023-00721-y.

[9] D. Progonov, V. Cherniakova, P. Kolesnichenko, and A. Oliynyk, "Behavior-based user authentication on mobile devices in various usage contexts," *EURASIP Journal on Information Security*, vol. 2022, Art. no. 6, 2022, doi: 10.1186/s13635-022-00132-x.

[10] S. Xiao, L. Zhang, Z. Tian, S. Su, J. Qiu, and R. Guo, "Pheromone-based graph embedding algorithm for Ethereum phishing detection," *Computer Networks*, vol. 260, Art. no. 111123, 2025, doi: 10.1016/j.comnet.2025.111123.

[11] A. Khan, "Graph Analysis of the Ethereum Blockchain Data: A Survey of Datasets, Methods, and Future Work," in *Proc. 2022 IEEE Int. Conf. Blockchain (Blockchain)*, 2022, pp. 250–257, doi: 10.1109/Blockchain55522.2022.00042.

[12] L. Wang, M. Xu, and H. Cheng, "Phishing scams detection via temporal graph attention network in Ethereum," *Information Processing & Management*, vol. 60, no. 4, Art. no. 103412, 2023, doi: 10.1016/j.ipm.2023.103412.

[13] J. Sun, Y. Jia, Y. Wang, Y. Tian, and S. Zhang, "Ethereum fraud detection via joint transaction language model and graph representation learning," *Information Fusion*, vol. 120, Art. no. 103074, 2025, doi: 10.1016/j.inffus.2025.103074.

[14] X. Pu, R. Jiang, Z. Song, Z. Liang, and L. Yang, "A medical big data access control model based on smart contracts and risk in the blockchain environment," *Frontiers in Public Health*, vol. 12, Art. no. 1358184, 2024, doi: 10.3389/fpubh.2024.1358184.

[15] R. Yaswanth, B. Pathakamuri, P. U. Sree, P. F. Khan, and A. G. Reddy, "Secure IPFS-based File Storage with Blockchain-Enabled Authentication, Access Control, and Secure Data Transfer," in *Proc. 4th Int. Conf. Inventive Computing and Informatics (ICICI)*, 2026, doi: 10.1109/ICICI68773.2026.11580430.

[16] N. Wu, L. Xu, and L. Zhu, "A blockchain based access control scheme with hidden policy and attribute," *Future Generation Computer Systems*, vol. 141, pp. 186–196, 2023, doi: 10.1016/j.future.2022.11.006.

[17] R. Singh, D. Kukreja, and D. K. Sharma, "Blockchain-enabled access control to prevent cyber attacks in IoT: Systematic literature review," *Frontiers in Big Data*, vol. 5, Art. no. 1081770, 2023, doi: 10.3389/fdata.2022.1081770.

[18] P. Bagga, A. K. Das, V. Chamola, and M. Guizani, "Blockchain-envisioned access control for Internet of Things applications: A comprehensive survey and future directions," *Telecommunication Systems*, vol. 81, no. 1, pp. 125–173, 2022, doi: 10.1007/s11235-022-00938-7.

[19] Z. Yan, X. Zhao, Y. Liu, and X. Luo, "Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda," *Information & Management*, vol. 61, no. 7, Art. no. 104026, 2024, doi: 10.1016/j.im.2024.104026.

[20] H. Agrawal, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L. Kulkarni, "Blockchain aware decentralized identity management and access control system," *Measurement: Sensors*, vol. 31, Art. no. 101032, 2024, doi: 10.1016/j.measen.2024.101032.

[21] J. Chen, U. Hengartner, and H. Khan, "MRAAC: A Multi-stage Risk-aware Adaptive Authentication and Access Control Framework for Android," *ACM Transactions on Privacy and Security*, vol. 27, no. 2, Art. no. 17, pp. 1–30, 2024, doi: 10.1145/3648372.

[22] X. Zhou, W. Yang, and X. Tian, "Detecting phishing accounts on Ethereum based on transaction records and EGAT," *Electronics*, vol. 12, no. 4, Art. no. 993, 2023, doi: 10.3390/electronics12040993.

[23] R. Alboqmi, S. Jahan, and R. F. Gamble, "A Risk Adaptive Access Control Model for the Service Mesh Architecture," in *Proc. 2024 IEEE 3rd Int. Conf. Computing and Machine Intelligence (ICMI)*, 2024, doi: 10.1109/ICMI60790.2024.10585800.

[24] C. Cholevas, E. Angeli, Z. Sereti, E. Mavrikos, and G. E. Tsekouras, "Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey," *Algorithms*, vol. 17, no. 5, Art. no. 201, 2024, doi: 10.3390/a17050201.

[25] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," *Blockchain: Research and Applications*, vol. 5, no. 3, Art. no. 100207, 2024, doi: 10.1016/j.bcra.2024.100207.

[26] H. Zhang, Y. Li, T. Zhu, C. Han, S. Wen, and Y. Xiang, "A scalable and semi-supervised approach for Ethereum fraud detection using Graph Neural Networks and K-Nearest Neighbors clustering," *Journal of Information Security and Applications*, vol. 95, Art. no. 104255, 2025, doi: 10.1016/j.jisa.2025.104255.

[27] M. Ghosh, R. Halder, and J. Chandra, "TREAT: Temporal and Relational Attention-Based Tensor Representation Learning for Ethereum Phishing Users," *IEEE Transactions on Services Computing*, vol. 18, no. 3, pp. 1838–1851, 2025, doi: 10.1109/TSC.2025.3568277.

[28] J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang, and Z. Zheng, "Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 37–49, 2023, doi: 10.1109/OJCS.2023.3245801.

[29] S. Sahoo, R. Halder, and S. Mondal, "Anomaly-free federated access control policy enforcement framework for Ethereum," *Cluster Computing*, vol. 28, no. 13, Art. no. 818, 2025, doi: 10.1007/s10586-025-05320-1.

[30] A. Xiong, Y. Tong, C. Jiang, S. Guo, S. Shao, J. Huang, W. Wang, and B. Qi, "Ethereum phishing detection based on graph neural networks," *IET Blockchain*, vol. 4, no. 3, pp. 226–234, 2023, doi: 10.1049/blc2.12031.