INTERNATIONAL JOURNAL OF NETWORKS AND SECURITY
(ISSN: 2693-387X)
VOL.06 ISSUE 02 (2026)

Research Article

Adaptive JWT Security Using Token Binding and Continuous Contextual Verification

Nguyen Minh Khoa [1]

[1]Faculty of Emerging Engineering Systems, Vietnam Institute of Technology, Vietnam

Abstract

JSON Web Token (JWT) authentication has become an important mechanism for stateless authorization because it enables distributed systems to carry verifiable identity and authorization claims without requiring continuous server-side session storage. However, conventional JWT validation primarily establishes whether a token is structurally valid, cryptographically authentic, and within its validity period. Such validation does not necessarily establish whether the token is still being used by the legitimate client, whether its contextual conditions remain trustworthy, or whether its use is consistent with the circumstances under which it was issued. This paper proposes an adaptive security model that combines JWT token binding with continuous contextual verification. The proposed approach treats authentication as a continuously evaluated security state rather than a one-time validation event. Token binding associates the token with a legitimate client or cryptographic context, while contextual verification evaluates factors such as device characteristics, request behavior, network context, session continuity, and access patterns. The methodology develops a conceptual architecture consisting of token issuance, binding, contextual assessment, adaptive risk evaluation, authorization enforcement, and token lifecycle management. The analysis further draws theoretical parallels from blockchain-based trust, smart-contract-enabled identity processes, data-integrity mechanisms, and decentralized security architectures. Findings indicate that combining cryptographic token association with continuous contextual assessment can reduce the security exposure associated with token theft, replay, and context changes, although implementation complexity, privacy considerations, interoperability, and false-positive decisions remain significant limitations.

Keywords: JWT Security, Token Binding, Continuous Authentication, Contextual Verification, Adaptive Authentication, Access Control, Risk-Based Authorization, Identity Security, Token Replay

check for updates

Received: 12 June 2026
Revised: 2 July 2026
Accepted: 20 August 2026
Published: 03 September 2026

Doi:10.55640/ijns-06-02-03

Page No: 31-39

INTRODUCTION

Legacy Modern distributed applications increasingly depend on token-based authentication to support scalable access across web applications, APIs, microservices, cloud environments, and mobile clients. JWTs are particularly useful because a digitally signed token can carry authentication and authorization information between independently deployed components. This architecture reduces dependence on centralized session state and can support highly distributed application environments. Nevertheless, the security properties of a JWT are strongly influenced by how the token is issued, protected, transported, validated, and revoked.

A fundamental limitation of conventional token authentication is the distinction between token validity and user legitimacy. A validly signed JWT proves that the token was generated by a trusted issuer and has not been altered. It does not, by itself, prove that the current presenter is the legitimate entity to which the token was originally issued. Consequently, token theft can transform a valid authentication artifact into an unauthorized access mechanism. This problem becomes more significant when tokens have relatively long lifetimes or when multiple services accept the same authorization token.

The broader literature on digital trust demonstrates the importance of preserving integrity and establishing stronger relationships between identities, transactions, and trusted environments. Blockchain research, for example, emphasizes distributed integrity and trust mechanisms in financial and communication environments (Treleaven, Brown, & Yang, 2017; Ali, Ally, & Dwivedi, 2020). Similarly, smart-contract-based identity processes demonstrate how identity-related decisions can be connected to programmable verification mechanisms (Kapsoulis et al., 2020). These principles provide useful theoretical foundations for reconsidering JWT authentication as more than simple signature verification.

Token binding provides one mechanism for addressing the ownership problem. Instead of treating a JWT as an independently transferable bearer artifact, the authentication architecture can associate its use with a cryptographic client context. If an attacker obtains the token but cannot reproduce the required binding proof, token replay becomes substantially more difficult. Ganapathy (2025) specifically positions token binding and contextual verification as mechanisms for strengthening JWT authentication, providing a direct foundation for the adaptive model proposed in this study.

The second mechanism is continuous contextual verification. Rather than making an authentication decision only when a token is initially presented, the system periodically or transactionally evaluates whether the surrounding conditions remain consistent with legitimate use. A request originating from a recognized device and expected network environment may receive a low risk assessment, whereas an otherwise valid token suddenly used from an unfamiliar device, unusual location, or anomalous access pattern may trigger additional verification or token restriction.

The objective of this paper is therefore to develop a conceptual framework for adaptive JWT security that integrates token binding with continuous contextual verification. The study focuses on the architectural logic, security benefits, operational trade-offs, and theoretical implications of this approach. It does not claim experimental performance measurements; rather, it provides a research-driven conceptual model that can serve as a foundation for subsequent implementation and empirical evaluation.

LITERATURE REVIEW

The literature supplied for this study does not focus exclusively on JWT authentication. Instead, it provides complementary evidence concerning digital trust, blockchain integrity, programmable authorization, distributed identity processes, and security-sensitive communication. Synthesizing these sources helps establish the theoretical foundation for adaptive JWT security.

Treleaven, Brown, and Yang (2017) examine blockchain technology within finance and emphasize the significance of distributed technological mechanisms for financial processes. Their work is relevant to JWT security at the architectural level because modern authentication systems similarly require mechanisms that preserve trust across multiple independently operating services. However, blockchain-based trust and JWT authentication are not equivalent: blockchain emphasizes distributed records and

consensus, whereas JWT security generally depends on cryptographic signing and issuer-controlled validation.

Ali, Ally, and Dwivedi (2020) provide a systematic review of blockchain technology in financial services. Their work highlights the broad role of blockchain in transforming information management, trust, and transaction processes. For adaptive JWT architecture, the important theoretical implication is that security should be evaluated as a system-level property rather than as an isolated cryptographic operation. Token verification, device trust, contextual signals, and authorization decisions should therefore operate as interconnected components.

Arslanian and Fischer (2019) characterize blockchain as an enabling technology for financial transformation. This perspective supports the use of enabling security mechanisms rather than relying on a single defensive control. Token binding can similarly be interpreted as an enabling mechanism: it does not replace JWT authentication but strengthens the relationship between a credential and its legitimate execution environment.

Dhanda and Garg (2021) discuss blockchain-enabled privacy and access control in the stock market context. Their work is particularly relevant to the authorization dimension of the proposed architecture. Authentication establishes who or what is requesting access, while access control determines what that entity should be permitted to do. Adaptive JWT security must therefore connect token validation with contextual authorization rather than treating successful authentication as sufficient for unrestricted access.

Kapsoulis et al. (2020) investigate KYC implementation using smart contracts within a privacy-oriented decentralized architecture. Their work demonstrates how identity verification can be represented as a structured, programmable process. This supports the theoretical positioning of continuous contextual verification as an ongoing policy process rather than a single binary authentication event.

Knezevic (2018) examines blockchain's impact on financial and other industries, reinforcing the broader argument that security architectures increasingly need to accommodate interconnected digital environments. Lamberti et al. (2018), through the application of blockchain, smart contracts, and sensors to insurance, further illustrate the value of combining transactional logic with contextual data. This is particularly relevant to contextual authentication because device and environmental signals can potentially contribute to adaptive security decisions.

Frikha et al. (2021) examine blockchain consensus algorithms in embedded architecture. Their study highlights the relationship between security mechanisms and constrained or specialized computing environments. For JWT systems, this creates an important design consideration: continuous verification cannot impose unlimited computational or communication overhead, particularly on mobile, IoT, and embedded clients.

Vallabhaneni (2021) addresses blockchain-enabled wireless communication with an emphasis on data integrity and privacy. This reinforces the importance of protecting communication environments in which authentication credentials are exchanged. Vallabhaneni (2024), addressing data breaches involving IoT devices, further demonstrates why credential security must be considered alongside endpoint and device security.

The most directly relevant source is Ganapathy (2025), which explicitly addresses strengthening JWT authentication through token binding and contextual verification. The proposed study extends this conceptual direction by organizing token binding and continuous contextual evaluation into an adaptive security architecture. The primary

research gap identified from the provided literature is therefore the lack of an integrated conceptual treatment that explains how binding, contextual signals, risk evaluation, and adaptive authorization can operate together as a continuous JWT security lifecycle.

METHODOLOGY

3.1 Research Design and Theoretical Positioning

This research adopts a conceptual architecture methodology rather than an empirical experimental methodology. The approach synthesizes the security principles represented in the supplied literature and translates them into an adaptive JWT security framework. The methodology is appropriate because the research objective is to explain how token binding and contextual verification can be integrated into a coherent authentication model.

The proposed architecture is based on two complementary security dimensions. The first is cryptographic possession control, represented by token binding. The second is contextual legitimacy, represented by continuous verification. A secure authentication decision is therefore modeled conceptually as:

Authentication Confidence = Token Integrity + Binding Validity + Contextual Trust

This does not represent a literal numerical formula; instead, it expresses the principle that token integrity alone should not determine access.

3.2 Adaptive JWT Security Architecture

The proposed framework consists of six functional stages: token issuance, token binding, contextual collection, continuous risk evaluation, adaptive enforcement, and token lifecycle management.

During token issuance, an authorization server authenticates the requesting entity and creates a JWT containing appropriate identity, audience, scope, issuer, and temporal claims. The token should be issued with the minimum privileges required for its intended purpose. This principle aligns with the access-control concerns evident in blockchain-enabled authorization research (Dhanda & Garg, 2021).

The second stage is token binding. A cryptographic relationship is established between the JWT and an authorized client context. Instead of relying solely on possession of the token, subsequent requests must demonstrate possession of the corresponding binding material. Conceptually, if an attacker copies the JWT but lacks the associated cryptographic key or proof mechanism, possession of the copied token should not be sufficient to authenticate.

This provides an important distinction between a conventional bearer token and a bound token. In the conventional model:

Valid Token → Potentially Valid Request

In the proposed model:

Valid Token + Valid Binding Proof + Trusted Context → Valid Request

Ganapathy (2025) provides the most direct theoretical basis for this combination of token binding and contextual verification.

3.3 Continuous Contextual Verification

The third stage evaluates contextual information associated with token use. Relevant signals may include device identity, client characteristics, network environment, access frequency, request timing, API behavior, session continuity, and changes in the operating context.

The objective is not to identify a person solely through environmental signals. Rather, contextual information functions as supporting evidence about whether the current token use remains consistent with previously established trust conditions. This approach reflects the broader security principle illustrated by sensor-integrated blockchain applications, where contextual information can influence the interpretation of transactions and contractual processes (Lamberti et al., 2018).

For example, assume a user obtains a JWT from a recognized device and uses it repeatedly to access an enterprise API. If the same token suddenly appears from an unfamiliar device and demonstrates an abnormal sequence of high-privilege API calls, the system should not automatically regard the token as trustworthy merely because its signature remains valid.

3.4 Contextual Risk Evaluation

The proposed model introduces an adaptive risk engine between authentication and authorization. The engine evaluates contextual evidence and classifies the request into conceptual security states such as trusted, uncertain, elevated-risk, or prohibited.

A low-risk request may proceed without additional interaction. A moderately suspicious request may require step-up authentication. A high-risk request may result in token suspension, session termination, or denial of sensitive operations.

This approach converts authentication from a static binary process into a dynamic decision system. Such a design is theoretically consistent with programmable verification approaches found in smart-contract-based identity systems (Kapsoulis et al., 2020), where predefined conditions can influence subsequent authorization behavior.

3.5 Adaptive Enforcement

The framework does not require every anomaly to result in immediate account termination. Instead, enforcement should be proportional to assessed risk. Low-risk anomalies may produce additional logging, moderate anomalies may restrict sensitive operations, and severe anomalies may invalidate the token or require complete reauthentication.

This proportionality is important because contextual verification inevitably produces uncertainty. Network changes, device updates, travel, mobile-network transitions, and legitimate changes in behavior can appear anomalous without representing attacks.

3.6 Token Lifecycle Management

Token security must also address issuance, renewal, expiration, revocation, and invalidation. Short-lived access tokens can limit the useful lifetime of stolen credentials, while refresh mechanisms can provide controlled continuity. Binding information should also be considered during refresh operations so that renewal does not unintentionally convert a bound authentication state into an unrestricted bearer credential.

The lifecycle perspective is consistent with the broader literature's emphasis on maintaining integrity and trust across evolving digital processes (Ali, Ally, & Dwivedi, 2020; Vallabhaneni, 2021).

3.7 Hypothetical Operational Example

Consider an enterprise API accessed from a registered employee laptop. The employee receives a JWT bound to a client cryptographic key. Normal requests from the registered device generate expected API patterns and therefore remain low risk.

Suppose an attacker extracts the JWT from application storage. The attacker attempts to replay it from another machine. The JWT signature remains valid, but the binding proof fails. The request is therefore rejected.

A more sophisticated scenario involves an attacker obtaining both a token and sufficient client information to imitate ordinary requests. Continuous contextual verification provides another defensive layer. A sudden change in device characteristics, request sequence, network context, and access volume can increase risk and trigger step-up authentication or token suspension.

The example demonstrates why the proposed architecture does not depend on a single control. Token binding protects the credential-to-client relationship, while contextual verification evaluates whether ongoing behavior remains consistent with legitimate use.

RESULTS

The conceptual analysis produces five principal findings.

First, JWT signature validation is insufficient as a complete security decision. A valid signature establishes token integrity and issuer authenticity, but it does not necessarily establish legitimate possession. The security distinction becomes particularly important when tokens operate as bearer credentials. Token binding addresses this limitation by requiring an additional cryptographic relationship between the credential and its authorized client.

Second, continuous contextual verification increases the depth of authentication assurance. A token's legitimacy can change during its lifetime because the environment in which it is used can change. Consequently, authentication should be capable of responding to contextual deviations rather than assuming that initial authentication remains permanently trustworthy. This finding directly corresponds to the conceptual direction identified by Ganapathy (2025).

Third, adaptive enforcement provides a more flexible response than binary authorization. Conventional systems often produce a simple accept-or-reject decision. The proposed architecture instead permits graduated controls, including unrestricted access, step-up authentication, restricted privileges, and token invalidation. This structure is theoretically consistent with broader access-control research emphasizing programmable and condition-based authorization (Dhanda & Garg, 2021; Kapsoulis et al., 2020).

Fourth, contextual security introduces a significant trade-off between protection and operational complexity. Device, network, behavioral, and environmental signals require collection, processing, storage, and policy interpretation. Excessive sensitivity can create false positives, while insufficient sensitivity can allow attacks to proceed. Therefore, contextual verification must be calibrated according to application risk rather than implemented as an indiscriminate monitoring mechanism.

Fifth, the proposed model is particularly relevant to distributed and heterogeneous environments. The supplied literature emphasizes blockchain, wireless communication, embedded systems, financial services, IoT, and decentralized architectures (Frikha et al., 2021; Vallabhaneni, 2021; Vallabhaneni, 2024). These environments frequently involve

multiple devices, services, and trust boundaries, making static credential validation increasingly inadequate.

However, the findings are conceptual rather than experimentally measured. No claims about specific detection percentages, latency improvements, or attack-prevention rates can be made without an implementation and controlled evaluation. The principal contribution is therefore an architectural model and set of testable security propositions rather than quantitative performance evidence.

DISCUSSION

The proposed framework changes the theoretical interpretation of JWT authentication from credential verification to continuous trust evaluation. This distinction is significant because modern attacks increasingly target credentials rather than attempting to forge cryptographic signatures. If a valid JWT is stolen, traditional validation mechanisms may correctly verify the token while incorrectly treating the attacker as legitimate. Token binding directly challenges this assumption by making possession of the token alone insufficient.

The combination with contextual verification creates a layered trust model. Cryptographic binding answers the question, "Is this request associated with the authorized credential context?" Contextual verification addresses a different question: "Does the current use remain consistent with legitimate behavior and conditions?" These questions are complementary rather than interchangeable. Ganapathy (2025) provides the direct conceptual basis for combining these mechanisms, while the broader literature supports the importance of integrity, programmable trust, and context-sensitive digital processes.

The model also has practical implications for enterprise API security. Organizations increasingly operate distributed applications in which a single identity may interact with numerous services. A token that remains valid across all services can become an attractive target after compromise. Adaptive authorization can reduce this exposure by restricting sensitive operations when contextual confidence decreases.

Nevertheless, stronger security introduces additional operational requirements. Context collection can create privacy concerns if organizations gather excessive environmental or behavioral information. A security architecture must therefore follow data minimization principles and clearly distinguish security-relevant signals from unnecessary surveillance. This concern is especially important when the proposed approach is deployed in IoT and wireless environments, where endpoint diversity and communication constraints are already substantial (Frikha et al., 2021; Vallabhaneni, 2021).

Another limitation concerns interoperability. Different applications may generate different contextual signals, and organizations may use heterogeneous identity providers, API gateways, and device-management platforms. A practical implementation therefore requires standardized interfaces between the token issuer, binding mechanism, contextual risk engine, and authorization layer.

False-positive decisions represent another significant trade-off. Legitimate users may change devices, networks, geographic environments, or normal behavior. A rigid contextual model could unnecessarily block legitimate access. Conversely, an overly permissive model could reduce the security benefits of continuous verification. The optimal design therefore requires calibrated risk policies, application-specific thresholds, and mechanisms for safe recovery.

The literature concerning blockchain-enabled security also highlights a broader architectural lesson. Distributed trust mechanisms can strengthen integrity, but they do not automatically solve every security problem. Blockchain, token binding, and contextual verification should therefore be viewed as complementary architectural concepts rather than interchangeable technologies (Ali, Ally, & Dwivedi, 2020; Arslanian & Fischer, 2019). The proposed JWT framework similarly avoids dependence on a single security mechanism.

The principal theoretical contribution is the integration of credential integrity, client binding, contextual confidence, and adaptive authorization into one continuous security lifecycle. Future empirical research should implement the framework and evaluate token-replay resistance, detection accuracy, authentication latency, resource consumption, false-positive rates, and usability under realistic attack scenarios. Such testing would establish whether the conceptual benefits identified here translate into measurable security improvements.

CONCLUSION

JWT authentication provides an efficient foundation for distributed authorization, but conventional token validation does not completely address the security risks associated with credential theft, replay, and changing usage contexts. This paper proposed an adaptive JWT security architecture that combines token binding with continuous contextual verification to address these limitations.

The proposed model establishes multiple layers of trust. Token binding strengthens the relationship between a JWT and its legitimate client context, while continuous contextual verification evaluates whether ongoing token use remains consistent with expected security conditions. An adaptive risk engine then converts contextual evidence into proportionate authorization actions, ranging from normal access to step-up authentication, restriction, or token invalidation.

The analysis demonstrates that this approach is theoretically aligned with broader research on digital integrity, programmable access control, decentralized identity processes, wireless communication security, and IoT data protection. At the same time, the framework introduces important challenges involving privacy, computational overhead, interoperability, false positives, and policy calibration.

The study's principal contribution is therefore a conceptual shift from static JWT validity toward continuous authentication confidence. Future research should develop a prototype and conduct controlled experiments involving token replay, device compromise, contextual anomalies, API abuse, and legitimate environmental changes. Quantitative evaluation of detection accuracy, latency, resource utilization, and usability would provide the empirical foundation necessary to validate and refine the proposed adaptive security model.

REFERENCES

1. Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management,54,102199.

2. Arslanian, H., & Fischer, F. (2019). Blockchain as an enabling technology. InThe Future of Finance (pp. 113-121). Palgrave Macmillan, Cham.

3. Dhanda, N., & Garg, A. (2021). Revolutionizing the Stock Market With Blockchain. In Revolutionary Applications of Blockchain-Enabled Privacy and Access Control(pp. 119-133). IGI Global.

4. Frikha, T., Chaabane, F., Aouinti, N., Cheikhrouhou, O., Ben Amor, N., & Kerrouche, A. (2021). Implementation of Blockchain Consensus Algorithm on Embedded Architecture. Security and Communication Networks,2021.

5. Ganapathy, S. K. (2025). Strengthening JWT Authentication Through Token Binding and Contextual Verification. Frontiers in Emerging Engineering & Technologies, 2(05), 15–23. Retrieved from https://irjernet.com/index.php/feet/article/view/jwt-authentication-security

6. Kapsoulis, N., Psychas, A., Palaio krassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. Future Internet,12(2), 41.

7. Knezevic, D. (2018). Impact of blockchain technology platform in changing the financial sector and other industries. Montenegrin Journal of Economics,14(1), 109-120.

8. Lamberti, F., Gatteschi, V., Demartini, C., Pelissier, M., Gomez, A., & Santamaria, V. (2018). Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage. IEEE Consumer Electronics Magazine,7(4), 72-81.

9. Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. Computer,50(9), 14-17.

10. Vallabhaneni, R. (2021). Blockchain-Enabled Wireless Communication: Revolutionizing Data Integrity and Privacy in Network Systems.

11. Vallabhaneni, R. (2024). Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices.