Journal of
Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.067360

REVIEW

Review of Communication Protocols and Cryptographic Techniques Applied in Secure Token Transmission

Michael Juma Ayuma[1,*], **Shem Mbandu Angolo**[1], **Philemon Nthenge Kasyoka**[2] **and Simon Maina Karume**[3]

[1]Department of Computer Science and Information Technology, School of Computing and Mathematics, The Co-Operative University of Kenya, Karen, Nairobi, P.O. Box 24814-00502, Kenya
[2]School of Science and Computing, South Eastern Kenya University, Kitui, P.O Box 170-90200, Kenya
[3]Department of Computer Science and Information Technology, Kabarak University, Nakuru, P.O Box 15232-20100, Kenya

*Corresponding Author: Michael Juma Ayuma. Email: ayumajuma@gmail.com

Received: 01 May 2025; Accepted: 21 July 2025; Published: 02 September 2025

ABSTRACT: Token transmission is a fundamental component in diverse domains, including computer networks, blockchain systems, distributed architectures, financial transactions, secure communications, and identity verification. Ensuring optimal performance during transmission is essential for maintaining the efficiency of data in transit. However, persistent threats from adversarial actors continue to pose significant risks to the integrity, authenticity, and confidentiality of transmitted data. This study presents a comprehensive review of existing research on token transmission techniques, examining the roles of transmission channels, emerging trends, and the associated security and performance implications. A critical analysis is conducted to assess the strengths, limitations, and applicability of various methods across different use cases, while identifying key advancements and enduring challenges. The findings aim to support researchers, practitioners and policymakers in selecting appropriate token transmission strategies and to provide a foundation for future innovations in this critical area.

KEYWORDS: Security protocols; token; encryption; blockchain; cryptography; token transmission

1 Introduction

Authentication tokens are used to verify that a user is authorized to access a given service, thereby granting permission accordingly [1]. These tokens enhance security by providing an additional layer of authentication, distinct from traditional passwords.

Authentication tokens have been implemented in various ways, largely due to their ability to carry data within the authorization process. For instance, JavaScript Object Notation (JSON) Web Tokens (JWTs) with Hash-based Message Authentication Codes (HMAC) are a common example [2]. Tokens play a critical role in multi-factor authentication (MFA), a security model that requires users to present multiple credentials from different categories to gain access [3].

MFA introduces an added layer of protection by verifying the legitimacy of devices and users. These authentication factors can include biometrics, passwords, tokens and more. The zero-trust security framework, which assumes that all devices may be compromised, mandates continuous authentication of all devices connected to the network [4]. Tokens can be generated based on user session IDs and other related parameters, as seen in the Cross-Site Request Forgery Machine Learning Shield (CSRF ML-SHIELD).

This system uses tokens to validate cross-origin requests, to reject unauthorized ones. Tokens are also employed in Single Sign-On (SSO) systems, where users authenticate once with a token issued by an identity provider to gain access to multiple services [5]. Furthermore, tokens are utilized in secure communication protocols such as Transport Layer Security (TLS), where they participate in stateless, one-time authenticated session resumptions during the TLS handshake process [6]. These use cases highlight the effectiveness of tokens in ensuring secure and mutual authentication across a range of applications.

A common example is the One-Time Password (OTP), a secure, time-sensitive code generated for a single authentication session. OTPs enhance security by limiting the window for unauthorized access. Although both OTPs and Personal Identification Numbers (PINs) serve authentication purposes, they differ significantly in structure and application. OTPs are usually dynamic, alphanumeric, and expire after a short period or a single use. In contrast, PINs are typically static, numeric and reused across sessions. PINs often range from 4 to 12 digits depending on the system.

Choosing between short and long PINs involves balancing usability and security. Short PINs (e.g., 4 digits) are easy to remember and quick to input, improving user convenience. However, they offer weak security, as only 10,000 combinations exist, making them susceptible to brute-force attacks. Users often exacerbate this risk by selecting predictable combinations.

Longer PINs (6–12 digits) significantly increase the number of possible combinations, making brute-force attacks far less feasible. For instance, a 12-digit PIN offers a substantially more secure barrier. However, long PINs can be challenging for users to remember and input, leading to usability issues. This may prompt users to adopt insecure practices, such as writing down their PINs or choosing easily guessable numbers.

To strengthen PIN-based authentication systems, tokens are often introduced as an additional security measure. A token—whether a physical device or a software application—generates a unique code used in conjunction with a PIN or password. This method aligns with the two-factor authentication (2FA) model, which combines something the user knows (a PIN/password) with something the user possesses (the token). Even if an attacker obtains the user's PIN, they would still need the token, which is not easily duplicated or guessed, thus reinforcing overall security.

Digital token transmission is a critical process that has significant implications for financial inclusion. In regions where traditional banking infrastructure is lacking, especially in developing countries, digital tokens enable individuals to participate in the global economy without direct interaction with banks.

Tokens may take the form of hardware devices that generate new OTPs every few seconds or software applications installed on smartphones. When combined with PINs, tokens create an effective safeguard against unauthorized access. This two-factor model mitigates risks associated with phishing, keylogging and stolen credentials. Even if the PIN is compromised, the absence of the corresponding token prevents unauthorized entry.

This study investigates various methods used to transmit digital tokens, evaluating their effectiveness, security, and applicability across different domains. It not only analyzes the structural characteristics of these methods but also their operational mechanisms. Special attention is given to the security capabilities of each technique in preventing fraud, hacking, and unauthorized access. The analysis encompasses cryptographic measures and other security defenses, focusing on the functionality, effectiveness and efficiency of token transmission techniques.

2 Motivation

This study is driven by the growing need for secure, efficient, and reliable token transmission mechanisms across critical domains such as blockchain, financial services, healthcare, the Internet of Things (IoT), and secure communications. As tokens play an increasingly central role in authentication, authorization, and digital asset representation, any interception or tampering with these tokens can result in serious security breaches. In light of the constantly evolving threat landscape, it is essential to analyze and assess existing communication protocols and cryptographic techniques to evaluate their effectiveness in terms of security, efficiency, scalability, and applicability to diverse use cases. This study seeks to provide a comprehensive resource for researchers, developers, and policymakers, guiding the selection and enhancement of secure token transmission strategies.

3 Contribution

This work reviews the foundational schemes developed and refined over decades of advancement in the field of information security, with particular emphasis on the mechanisms that ensure the secure transmission of tokens within communication networks. The main contributions of this paper are as follows:

1. Comprehensive analysis of communication protocols commonly employed in secure token transmission. The study evaluates how these protocols uphold confidentiality, integrity, and authenticity of transmitted data, highlighting their respective strengths and limitations.
2. Examination of cryptographic techniques used to protect tokens during transmission. This includes both symmetric and asymmetric encryption methods—such as RSA, AES and elliptic curve cryptography (ECC)—as well as hashing algorithms and digital signatures. The effectiveness of these techniques in mitigating various attacks is critically assessed.
3. Integration of cryptographic protocols with token-based authentication systems. The paper explores how incorporating cryptographic methods enhances the security of token transmission by preventing interception, duplication and tampering.
4. Identification of potential vulnerabilities and attack vectors. By analyzing real-world scenarios—including token theft, session hijacking, and token forgery—The study highlights security gaps in existing communication protocols and cryptographic mechanisms.
5. Recommendations for improving token transmission security. Drawing from the analysis of current practices and their limitations, the paper offers practical recommendations to enhance both the security and efficiency of token-based systems. These suggestions aim to bridge existing gaps while supporting scalability.
6. Future research directions. The paper synthesizes the current state of secure token transmission systems and explores emerging technologies, offering insights into areas that require further investigation and development.

By addressing these critical aspects and offering a holistic view of information security, this paper positions itself as a valuable and distinctive resource. It aims to advance both the understanding and practical implementation of robust security measures in the evolving domain of information systems, serving the needs of researchers, developers and security practitioners seeking to strengthen token-based authentication systems.

4 Methodology

This survey employed a systematic literature review to assess secure token transmission. We focused on communication protocols and cryptographic techniques. First, we formulated hypotheses and mapped related work. Next, we collected peer-reviewed articles, technical reports and industry standards from leading academic databases. We then built a taxonomy of token-security methods and protocols. Each approach was evaluated on encryption strength, efficiency, latency, scalability, and other key metrics. Finally, we analyzed the results to identify emerging trends, common practices, and research gaps. Based on these insights, we proposed recommendations to bolster token-transmission security across diverse application domains. During the preparation of this manuscript, OpenAI's ChatGPT was used for language refinement purposes, including improving grammar, clarity, and sentence structure. The tool was not involved in the generation of scientific ideas, data analysis, or the formulation of conclusions. All intellectual content, including research design, data interpretation, and conclusions, remains entirely the work of the authors.

4.1 Search Strategy

We conducted our search in IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Google Scholar, and comparable platforms. We looked specifically for studies on secure token transmission, related communication protocols, and cryptographic methods. We refined the query iteratively by adding or adjusting keywords. We screened titles and abstracts to focus on token-security issues. From the selected articles, we extracted additional terms to expand the search. This process followed the standardized review framework described in [7].

4.2 Keywords and Search Terms

To ensure breadth and relevance, we used these terms (and their combinations):

- secure token transmission
- communication protocols AND cryptography
- token security
- cryptographic techniques for token transmission
- token-based authentication
- secure communication protocols

4.3 Search Period

We limited our review to publications from 2018 through 2025. This range captured the latest advances and addressed current security challenges in token transmission.

4.4 Initial Results

The initial search returned over 2300 records. These covered a spectrum of topics, including token transmission architectures, encryption algorithms, and protocol analyses.

4.5 Inclusion and Exclusion Criteria

We applied strict criteria to maintain focus and quality:

Inclusion Criteria:

1. Peer-reviewed journal articles or conference papers.

2. Studies on communication protocols, cryptographic techniques or secure token transmission.

3. Publications in English.

Exclusion Criteria:

1. Non-peer-reviewed materials (e.g., editorials, white papers).

2. Works unrelated to token security or cryptographic methods.

3. Papers focused exclusively on legal, financial or policy aspects without technical analysis.

4.6 Refinement Process

We refined the corpus in three stages:

1. *Title and Abstract Screening:* We reviewed over 2300 titles and abstracts. We retained 537 papers that aligned with our focus.

2. *Full-Text Review:* We performed detailed evaluations of those 537 papers, narrowing the set to 152 technically relevant studies.

3. *Final Selection:* Applying our inclusion criteria to the 152 studies yielded 166 papers for in-depth analysis.

4.7 Thematic Grouping

We organized the final selection into six thematic areas:

1. *Token Types:* Hardware vs. software tokens and their authentication roles.

2. *Transmission Protocols:* Secure channels such as SSL/TLS and IPsec, and their effectiveness in preserving data confidentiality and integrity.

3. *Cryptographic Algorithms:* Symmetric (e.g., AES) and asymmetric (e.g., RSA, ECC) encryption, hashing, and digital signatures.

4. *Application Domains:* Implementation challenges in e-commerce, online banking, cloud services, and IoT.

5. *Vulnerabilities:* Token theft, session hijacking, and man-in-the-middle attacks.

6. *Mitigation Techniques:* Multi-factor authentication, advanced cryptographic protocols, and hybrid security models.

This rigorous approach provided a thorough and structured evaluation of token-transmission methods, as shown in Fig. 1 below. It exposed key security vulnerabilities and revealed promising directions for future research.

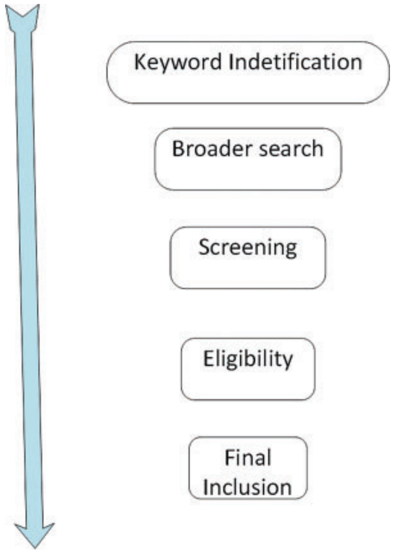

Figure 1: Flow reflecting the search process

5 Applications of Tokens and Their Importance

One-time passwords (OTPs) play a crucial role in strengthening user authentication. Because each OTP is valid for a single session, it offers greater security than static passwords. This approach thwarts phishing attacks and addresses vulnerabilities inherent in traditional password systems [8]. After entering a username and password, users must supply the OTP—typically delivered via a mobile app or physical device. This two-factor authentication process remains secure even if an attacker obtains the user's password. Cryptographic methods and robust data-exchange mechanisms ensure that token transmission is safe, efficient, and reliable.

Digital tokens are widely adopted in online banking and e-commerce to protect consumers. By enabling direct transactions between buyers and sellers, tokens eliminate intermediaries and reduce transaction costs.

In healthcare, tokens help secure patient data through blockchain-based systems that prevent unauthorized access. For example, a blockchain anti-fraud framework allows patients to act as validating nodes for claims and transaction records. This increases transparency, engages patients in verification, and reduces healthcare fraud and abuse [9]. Secure Socket Layer (SSL) protocols further protect electronic health records and other sensitive information during transmission, especially when large amounts of data travel across potentially compromised networks [10].

JSON Web Tokens (JWTs) have become a standard for safeguarding user identity in web applications. JWTs provide a reliable, scalable method for distributed access control [11]. Even if an attacker discovers a user's credentials, the JWT prevents unauthorized access to the account.

In supply chain management, tokens trace the origin and movement of goods, enhancing the credibility of the entire value chain [12]. Similarly, in digital identity systems, token transmission supports self-sovereign identity. Individuals hold their own identity keys and selectively share personal data with service providers [13]. This empowers citizens to control their data and maintain privacy.

6 Types of Tokens

Tokens are diverse digital representations used across various systems to serve different purposes, including authentication, security, access control, and asset representation. In the following sections, we will explore specific types of tokens, each with unique characteristics and use cases, providing a deeper understanding of their roles in modern digital ecosystems.

6.1 Utility Tokens

Tokens grant users access to products or services within a specific platform and enable transactions there. For example, they can cover transaction fees, unlock premium features, or allow users to participate in platform governance [14]. This role is most pronounced in Decentralized Finance (DeFi), where utility tokens support a wide range of financial services without intermediaries, resulting in greater efficiency and lower transaction costs [15]. Consequently, tokens are essential to blockchain ecosystems because they foster user engagement and interaction.

6.2 Security Tokens

A security token represents a tangible asset, such as company shares, debt instruments, or property, in digital form [16]. These tokens grant investors rights like dividends or voting privileges and are subject to securities regulations. By integrating smart contracts, compliance can be automated so that only accredited investors can purchase the tokens and all sale processes are recorded on the blockchain. This automation enhances efficiency and reduces errors and fraud. For example, in real estate, security tokens enable fractional property ownership, improving investment accessibility and liquidity. In equity markets, companies issue tokens to represent shares, facilitating capital raising and fractional ownership. Tokenized debt instruments, such as bonds, benefit from increased tradability and liquidity. Art and collectibles can also be tokenized, offering fractional ownership of high-value items and broadening investor participation. Smart contracts on these tokens automate regulatory compliance—such as enforcing accredited-investor rules and distributing dividends—further boosting efficiency and reducing fraud.

6.3 Payment Tokens

Payment tokens, or cryptocurrencies, serve as digital currencies for purchasing goods and services, remittances, or stores of value [17]. Examples include Bitcoin, Ethereum, and Litecoin. These tokens enable faster, cost-effective, and borderless transactions compared to traditional payment methods. They are widely used on e-commerce platforms, for international money transfers, and as components of investment portfolios. By reducing transaction fees and processing times, payment tokens improve the overall user experience and make global financial activities more accessible.

6.4 Non-Fungible Tokens (NFTs)

Non-fungible tokens (NFTs) are unique digital assets that prove ownership of a specific item or piece of content [18]. NFTs use cryptography and smart contracts to record ownership and enforce the terms of transfer automatically. They provide provenance and authentication for digital art, music, videos, virtual real estate, and collectibles. On platforms like OpenSea and Rarible, artists sell exclusive digital artworks as NFTs. In gaming, NFTs enable trading of rare characters or skins. Virtual worlds such as Decentraland and Cryptovoxels allow users to buy and sell tokenized land parcels. Smart contracts ensure the security, uniqueness, and traceability of each NFT.

7 Token Transmission

Digital tokens can be transferred between individuals via exchanges, over-the-counter trades, or smart contracts on blockchain platforms. Transfers may occur within the same blockchain network or across different chains, depending on the token type. Security is paramount because tokens and their ownership carry real value. Common security measures include data encryption during transmission, strong authentication mechanisms, and secure key management.

Authentication validates an entity's identity and legitimacy. It is the first line of defense in secure communication. Robust authentication protocols must resist attacks such as denial-of-service, side-channel exploits, forgery, parallel sessions, password guessing, and replay attacks. However, many protocols lack adequate defenses, creating vulnerabilities during transmission.

Before the adoption of sophisticated authentication, symmetric cryptosystems like the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) protected networks and hardware. Later, asymmetric systems—RSA, Elliptic Curve Cryptography (ECC), Diffie-Hellman key exchange, digital signatures, and identity-based cryptography—added further layers of security [4].

Real-time token-movement tracking enhances transparency in financial transactions and builds trust among participants [19]. Data integrity within tokens is maintained using digital signatures, such as HMAC-SHA256, which prevent unauthorized modifications [11]. Compliance with legal and market regulations is also critical to ensure the legitimacy of token transfers. Additional factors include transmission speed and efficiency, especially in financial contexts.

On the hardware side, Physically Unclonable Functions (PUFs) exploit microscopic variations in semiconductor devices to uniquely identify and authenticate hardware components. Secure device firmware protects the software layer; tampering with firmware can lead to cloning, modification, and other attacks [20].

During web-based transmission, using HTTPS encrypts token exchanges between client and server, protecting them from interception. Setting cookies as Secure and Http Only further guards tokens by ensuring they are only sent over encrypted channels and are inaccessible to client-side scripts, mitigating cross-site scripting (XSS) risks.

8 Security Considerations for Token Transmission

Protocol choice is critical in multi-node environments. For example, the Round-Robin protocol uses time-division multiple access to minimize data collisions during token passing [19]. In Wireless Sensor Networks (WSNs), multi-token strategies optimize energy usage and ensure collision-free communication.

Security protocols like JSON Web Tokens (JWTs) maintain data integrity and confidentiality during transmission [21]. In IoT systems, token-based authentication improves access control and reduces vulnerabilities to man-in-the-middle attacks [22]. E-commerce platforms also leverage tokenization to mitigate data-breach risks and unauthorized access 24 [23].

Innovations in token-passing, such as the multi-channel token passing (MCTP) system by Hsu and Liu, demonstrate how control-packet use can be optimized for modern networks [24]. Research on inter-blockchain communication shows that improving relay time boosts interoperability among blockchains [25].

Infrastructure security remains essential. Emerging technologies like quantum tokens and Tokenized Message Authentication Codes (TMAC) can delegate signing authority securely while ensuring strong authentication [26]. In federated identity and blockchain applications, decentralized authentication models using smart contracts offer enhanced security for Web 3.0 [27].

Future communication frameworks, such as 6G, will introduce new security challenges and requirements [28]. Token-based systems must defend against timing attacks on authentication protocols like FIDO2, which can compromise user privacy by linking accounts across services [29]. Effective solutions must balance robust security with seamless usability to maintain a positive user experience [30].

9 Communication Protocols and Methods of Token Transmission

The transmission of digital tokens involves multiple sophisticated procedures and diverse technologies to ensure secure and efficient token exchange. Protocols define the rules for transferring tokens between entities in a network. They also manage the order in which nodes transmit tokens to prevent collisions and reduce congestion, thereby enhancing data-exchange reliability [31]. Various token-transmission algorithms are in use, each with its own advantages and limitations. Standardized payload formats, message structures and APIs are essential to achieve a cohesive token economy [32]. Table 1 outlines Summary of these Protocols, description, use cases, merits and demerits in their applications.

9.1 Transport Layer Security (TLS)

Transport Layer Security (TLS) is a widely adopted cryptographic protocol that secures data transmission over computer networks. By encrypting and authenticating the data exchanged between parties, TLS prevents eavesdropping, tampering, and phishing attacks, making it indispensable for secure token exchange. Binding tokens to a TLS session further mitigates risks of token theft and replay attacks by ensuring each token is valid only within its original session context [33]. Mutual authentication schemes—such as OAuth 2.0's mutual-TLS client authentication—leverage this binding to verify both client and server identities [34].

Hypertext Transfer Protocol Secure (HTTPS) pairs HTTP with TLS to protect web-based token transactions. HTTPS encrypts token exchanges between clients and servers, safeguarding financial systems and other token-based services from interception and manipulation. When combined with elliptic curve cryptography and trusted token formats like JSON Web Token (JWT), TLS provides robust authentication of devices communicating with backend servers. This dual-layer security is especially important in Internet of Things (IoT) applications, where device integrity is critical [35].

TLS 1.3 enhances security by eliminating static RSA key exchanges, reducing handshake latency, and easing migration from older, more error-prone versions [6]. Older implementations, however, have suffered from vulnerabilities such as the Heartbleed bug in OpenSSL, which allowed attackers to steal private keys and session tokens from server memory [6]. Such flaws underscore the importance of rigorous protocol maintenance and patching.

Despite its strengths, TLS's complexity can lead to misconfigurations that expose tokens to interception or unauthorized access [36]. Implementation issues—ranging from flawed certificate validation to improperly configured cipher suites—can undermine TLS's protections. In man-in-the-middle (MITM) attacks, for example, an adversary can impersonate a server to capture and modify tokens in transit [37]. These threats are exacerbated when clients blindly trust compromised or misused TLS certificates, highlighting the need for strict certificate management and validation processes [36].

9.2 Inter-Blockchain Communication (IBC)

Inter-blockchain Communication (IBC) protocols enable seamless asset transfers across distinct blockchains without sacrificing security or privacy [25]. These protocols lock tokens on the source chain and mint equivalent tokens on the destination chain. Upon return, the destination tokens are burned and the original tokens are released.

However, IBC's modular design can introduce challenges. As the number of connected blockchains grows, communication overhead increases—particularly in Byzantine Fault Tolerant (BFT) systems that require extensive inter-node messaging [38]. This added traffic can degrade performance during periods of high transaction volume [39].

Reliance on third-party relayers also creates trust vulnerabilities. For example, the Open Digital Asset Protocol (ODAP) depends on multiple gateways, which can be targeted by malicious actors [40]. Cross-chain transactions often experience high latency due to varying authentication processes across heterogeneous chains. The absence of standardized protocols exacerbates these delays and raises transaction costs [41]. Such fragmentation hampers efficient token transfers and slows broader adoption of IBC solutions.

9.3 WebSocket

WebSocket is a protocol that supports full-duplex communication between clients and servers. It delivers real-time updates and enables secure token exchange with minimal delay [42]. This capability helps market participants respond swiftly to changing conditions, making digital-token markets more efficient and dynamic. WebSocket also has lower latency and overhead than traditional HTTP methods, which makes it ideal for high-performance, responsive applications [43].

A key security risk for WebSocket is man-in-the-middle (MitM) attacks, especially when SSL/TLS is missing or misconfigured [44]. Such vulnerabilities can expose sensitive tokens and compromise message integrity. Persistent WebSocket connections can also be exploited if session tokens lack strong protection or proper expiration, leading to token theft or replay attacks [45]. Finally, because WebSocket keeps connections open to continuously send data, it can be vulnerable to denial-of-service (DoS) attacks, where an adversary floods the channel and disrupts service [46].

9.4 Interledger Protocol (ILP)

This protocol provides a standard framework for linking one payment network and ledger to another. It enables straightforward token exchange between different blockchains, ensuring secure cross-border transfers between financial systems. By using Hashed Timelock Contracts (HTLCs), it guarantees that assets move atomically and securely across parties and platforms, resolving compatibility issues among diverse systems. This ensures that transactions are either fully completed or fully rolled back to maintain integrity, as shown in Fig. 2 [47]. Fig. 3 shows how this functionality is essential for atomic swaps and the support of efficient ledger management. Recent studies also highlight its role in the Interledger Protocol (ILP) for decentralized access control and asset management [48].

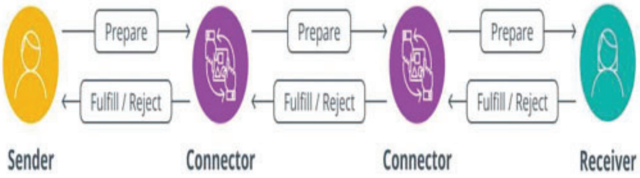

Figure 2: How packets facilitate value transfer across ledgers. Source: interleger.org

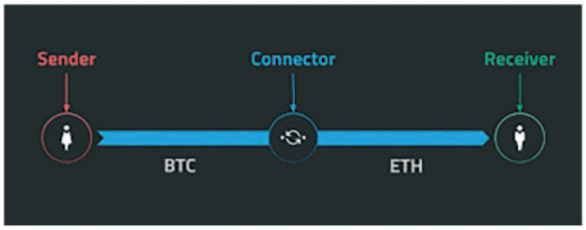

Figure 3: Swap Management of ILP

Recent protocol enhancements have improved scalability and performance but also raised concerns about transparency and trust in cross-border transactions [49]. One significant risk is timing attacks, which can exploit the anonymous, multi-hop locking mechanisms used during token transfers [50]. Two-way pegs also introduce vulnerability: a single compromised connector handling large volumes of data can jeopardize the entire transaction.

Secret sharing between parties further complicates security. If these secrets are not managed carefully, they can inadvertently expose token information [51]. Finally, the lack of strong cryptographic standards in many ledgers hinders interoperability and poses a barrier to efficient token transfers across diverse systems [50].

9.5 Message Queuing Telemetry Transport (MQTT)

Message Queuing Telemetry Transport (MQTT) is an extremely lightweight token-transmission technique designed for constrained devices and low-bandwidth networks. In this method, tokens are exchanged within Internet of Things (IoT) environments to enable device authentication and facilitate microtransactions. MQTT's low-overhead publish/subscribe model supports real-time messaging while minimizing bandwidth usage, making it ideal for resource-limited applications such as smart homes and industrial IoT deployments [52].

MQTT relies on three primary entities: the publisher, the subscriber, and the broker. The broker manages all message distribution and enforces token-based authentication by validating session-specific tokens before permitting publish or subscribe actions [53]. This mechanism ensures that only authorized devices participate in messaging and helps protect data from unauthorized access or tampering [54].

However, MQTT lacks built-in security features. Without additional layers such as Transport Layer Security (TLS), both data integrity and privacy remain at risk. The broker-centric architecture also introduces a single point of failure: if the broker is compromised, all connected clients become vulnerable to attacks like man-in-the-middle and replay exploits [55,56]. Furthermore, MQTT's dependence on TCP can introduce latency and performance challenges, particularly when scaling to large deployments [57]. Finally, many MQTT implementations omit proper encryption, allowing tokens to be intercepted or modified during transmission [58].

9.6 Peer-To-Peer (P2P)

Peer-to-peer (P2P) protocols enable fully decentralized operations by allowing nodes to communicate and exchange tokens directly, without a central server. In these networks, each participant acts as both client and server. For example, atomic cross-chain transactions let users swap assets between blockchains like Bitcoin and Ethereum without intermediaries [59].

P2P token exchange underpins decentralized applications and file-sharing platforms such as BitTorrent. The Bitcoin protocol itself uses P2P messaging to move tokens securely and reliably. This decentralization improves system resilience and reduces single points of failure in the digital economy.

However, P2P networks lack inherent trust between peers, which can lead to token theft, manipulation, and other fraud risks. New participants have no established reputation, increasing the chance of malicious actors joining the network. To address these challenges, robust trust and reputation management mechanisms are essential but difficult to implement [59].

P2P systems also face performance issues under heavy network load. Unpredictable peer bandwidth can cause delays in token transmission and higher latency, undermining the real-time benefits of peer-to-peer exchanges [60].

Table 1: A Summary of Protocols, description, use cases, merits and demerits in their applications

	Protocol	Description	Use Cases	Advantages	Disadvantages
1	**Transport Layer Security (TLS)**	A cryptographic protocol designed to provide secure communication over a computer network by ensuring confidentiality, integrity, and authentication.	Securing web traffic, online banking, and email communication.	Ensures data confidentiality and integrity, widely adopted for secure communication across the web.	Can introduce overhead, affecting performance and resource consumption; requires certificates and trust management.
2	**Inter-Blockchain Communication (IBC)**	A protocol enabling different blockchains to communicate and share data or assets between each other, improving interoperability across blockchain networks.	Enabling cross-chain interoperability for decentralized finance (DeFi) applications and blockchain ecosystems.	Enhances blockchain interoperability, facilitating communication between different blockchain ecosystems.	Still evolving and not yet fully standardized across all blockchain platforms, limiting adoption.
3	**WebSocket**	A communication protocol providing full-duplex communication channels over a single, long-lived TCP connection, ideal for real-time data exchange.	Real-time data feeds, online gaming, stock market tickers, and IoT applications.	Allows real-time, full-duplex communication with low latency, essential for interactive applications.	Not ideal for large-scale data transfer; may introduce delays if not properly managed.

(Continued)

Table 1 (continued)

	Protocol	Description	Use Cases	Advantages	Disadvantages
4	**Interledger Protocol (ILP)**	A protocol that facilitates seamless transfer of funds or assets across different payment networks, aiming to enable interoperability between payment systems.	Enabling payments, remittances, and cross-border transactions between different financial systems.	-Improves cross-network payment systems, making global transactions more efficient and accessible. -Addresses the issue of compatibility between various systems.	-vulnerable to timing attacks, especially when the token transfer is in the backdrop of anonymous multi-hop locks. Lacks full compatibility with all payment networks, limiting its universal application [61].
5	**Message Queuing Telemetry Transport (MQTT)**	A lightweight messaging protocol for small sensors and mobile devices, optimized for low-bandwidth, high-latency, or unreliable networks.	IoT devices, telemetry systems, remote sensing, and applications with constrained resources like energy or bandwidth.	Optimized for low-bandwidth environments, making it ideal for IoT and telemetry applications.	Not as widely adopted as other messaging protocols; can face integration challenges with existing systems. Compatibility issues may arise when deploying MQTT in existing infrastructures, often requiring significant changes to system architectures [62].

(Continued)

Table 1 (continued)

	Protocol	Description	Use Cases	Advantages	Disadvantages
6	**Peer-To-Peer (P2P)**	A network model that allows direct communication between peers without relying on a central server, enabling decentralized data exchange.	File sharing, decentralized applications, VoIP, and decentralized networks like blockchain-based systems.	Facilitates decentralized, secure, and direct communication between peers, reducing reliance on central servers.	Relies on peer discovery and security management, which can be complex and vulnerable to malicious attacks. -There's no trust between the peers; this is a primary concern since this can facilitate adversarial activities.
7	**HTTPS**	An extension of HTTP that provides secure communication by using encryption (TLS/SSL), ensuring data confidentiality, integrity, and authentication.	Securing web browsing, online shopping, and communication for sensitive transactions like banking and data transfers.	Provides encryption and authentication, ensuring secure data transmission over the web, and protecting against attacks.	Can incur performance costs due to encryption overhead; requires secure certificate management and trust systems.

10 Cryptographic Techniques Used in Token Transmission

To protect tokens during transmission—especially over public or untrusted networks—systems employ a range of cryptographic methods. This section reviews the primary techniques, including encryption, digital signatures, and hashing, and explains how each contributes to the confidentiality, integrity and authenticity of token data.

10.1 Symmetric Encryption

Symmetric encryption uses a single secret key for both encrypting and decrypting data, as depicted in Fig. 4. It delivers strong security with relatively low computational overhead compared to asymmetric methods. Because of its efficiency, symmetric encryption is widely adopted for securing data in transit and ensuring fast, reliable token transmission [63].

Advanced Encryption Standard (AES) enhances security by using keys of 128, 192, or 256 bits for token transmission [64]. AES is widely applied to encrypt token data in e-commerce and secure communications because it is computationally efficient and suitable for bulk encryption. However, symmetric encryption faces key distribution challenges: the sender and receiver must share the secret key over a secure channel, which is not always feasible [64]. Although symmetric algorithms are faster and less resource-intensive than asymmetric ones, the need to share keys increases the risk of key compromise and exposure, undermining their security benefits [65]. When multiple nodes use the same symmetric key, a single key breach can expose all transmitted data, endangering the entire network [66]. Moreover, AES does not include built-in mechanisms for key management or revocation, making it difficult to maintain long-term security in dynamic environments [65].

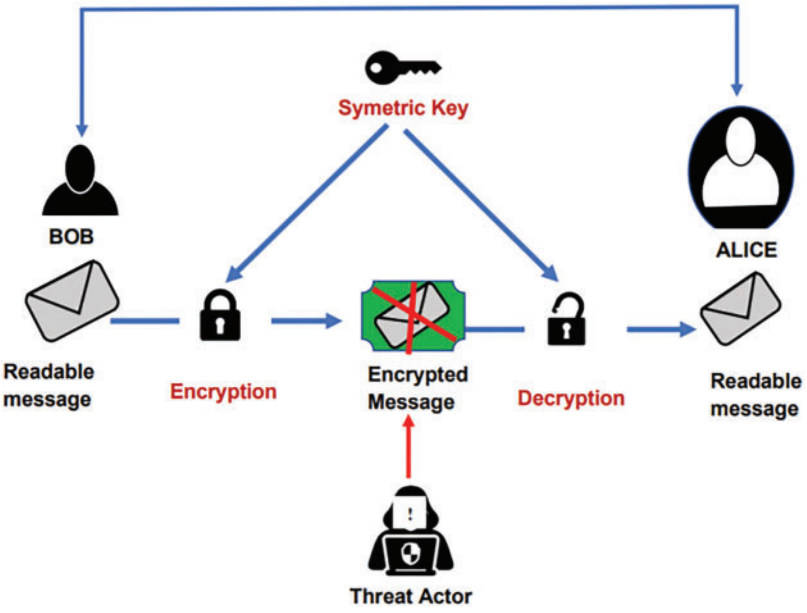

Figure 4: Symmetric encryption

10.2 Asymmetric Encryption

This algorithm creates a pair of keys: a public key for encryption and a private key for decryption. The public key is freely shared, while the private key remains secret with the recipient. Unlike symmetric encryption, this method does not require the sender and receiver to share a secret key in advance, thereby reducing the risk associated with key distribution. Fig. 5 illustrates a common principle used in Asymmetric encryption.

Two leading asymmetric encryption methods for token transmission are RSA and Elliptic Curve Cryptography (ECC). RSA is valued for its reliability and speed in securing data during transit [67]. Its security depends on the difficulty of factoring large prime numbers. In contrast, ECC achieves comparable security with much smaller key sizes, reducing CPU and memory demands. This efficiency makes ECC ideal for resource-constrained environments.

Asymmetric encryption is primarily used for key exchange and verifying the identities of communicating parties, rather than for bulk data encryption, which remains the domain of faster symmetric methods. Integrating asymmetric techniques into micro-application architectures enhances both authentication and authorization processes, thereby safeguarding token transmission [68]. Beyond token exchange, these methods secure data flows in diverse applications such as genomics and IoT systems [67].

However, asymmetric algorithms incur higher computational costs. Operations like RSA encryption and decryption introduce latency, which can be problematic on low-power devices [69,70]. Emerging threats also challenge the long-term viability of public-key schemes. For example, Shor's Algorithm can, in theory, break RSA and ECC by factoring or solving discrete logarithms in polynomial time [71]. Finally, key management remains critical: if a private key is compromised, all tokens and data protected by its matching public key become vulnerable [72].

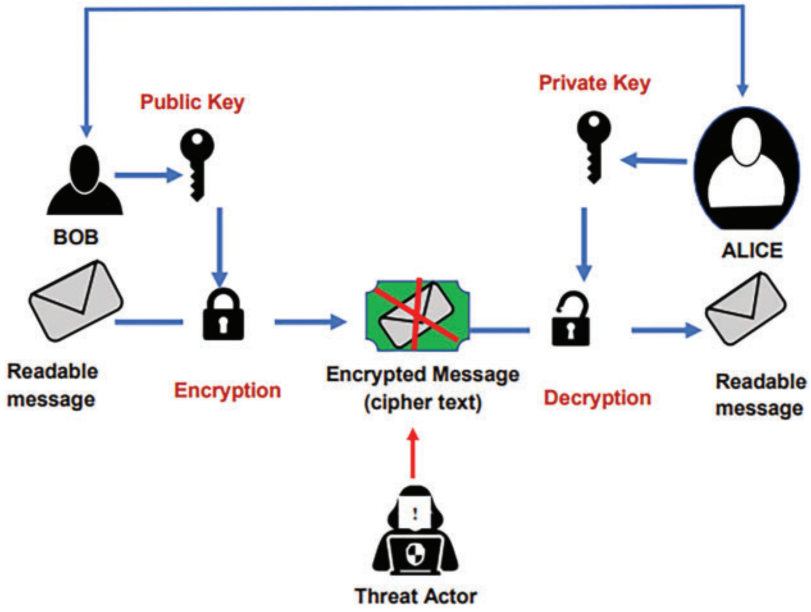

Figure 5: Asymmetric encryption

10.3 Digital Signatures

Token transmission is incomplete without considering digital signatures, which play a crucial role in verifying the authenticity of transmitted tokens. The technology behind digital signatures relies on asymmetric key encryption, such as RSA, enabling secure communication even over insecure channels [73].

A digital signature refers to the process of creating an exclusive digital code for a document using the sender's private key. This is achieved by hashing the document and encrypting it using a cryptographic algorithm, such as RSA or ECC. The signature that is generated out of this is, in turn, validated by the receiver by using the public key of the sender. In one way, if the verification process is successful, it validates the fact that the data was sent by the claimed sender of the message and has not been changed in the course of transmission. Digital signatures are a reliable security that is used to build up confidence between the communicating parties, especially in situations where the content of the data is very sensitive and needs to be protected against any manipulation, such as in e-commerce and contracts.

Nonetheless, the integrity and authenticity of the digital signatures depend mainly on the safeguarding of the private key. This means that if the private key associated with any person is in the wrong hands or with the adversary, the individual will be capable of forging signatures and hence forging messages, which compromises trust in the system. Tokenized Message Authentication Code (TMAC) presents a way of implementing authentication between two parties and applies the concepts applied in quantum cryptography [26]. This is accompanied by the creation of multiparty hash time-lock contracts (MP-HTLC) which makes the swapping of tokens across multiple blockchains possible and effective which employing the concept of secure multiparty computation [74].

The use of these technologies further salient changes in the area of digital signatures and, especially, their use in the transmission of secure tokens. However, they possess several vulnerabilities that defeat the efficiency of the token's transmission process. There is, however, one weakness that arises from the use of this protocol: they are prone to signature flooding attacks whereby the adversary floods most of the computational resources of the intended recipient, especially those operating under resource-limited environments such as mobile platforms. Further, the problem of hash collision is dangerous for data integrity because two different inputs may give the same hash value, thus endangering security measures related to the usage of signatures [75].

Another challenge is quantum attacks, which threaten many present-day digital signature algorithms because they are based on mathematical problems that are easy for quantum computers to solve [76]. Also, digital signatures are prone to man-in-the-middle attacks whereby an attacker arbitrates between two legitimate parties by masking and modifying the contents of transmission [77].

10.4 Hash Functions

Since tokens are transmitted as data, hash functions are used to verify the integrity of the data being transmitted. Hashing works by accepting an input, or a "message", and producing a string of bytes, normally referred to as the digest, that does not seem to have any pattern. It is very sensitive to any change in the input and provides a hash output that is different even after a minor input change, which makes it suitable for checking data integrity.

One of the most commonly used hash functions is SHA-256 (Secure Hash Algorithm 256-bit), which is adopted widely in several security protocols and blockchain technology. They are used in conventional cryptography to generate tokens for secure transmission. They are mostly used in timestamping services, which reveals their suitability in token generation that involves combining the input data with time stamps to generate tokens that can be compared with those stored in a public list [78]. This mechanism increases the strength of the digital tokens, for instance, in the NFT whose hash functions are important to ensure the uniqueness of the tokens [79].

One major risk stems from the improvements in terms of processing power and cryptanalysis, wherein hash algorithms that were relatively secure in the past are now easily compromised [80]. The former algorithms are compounded by the emerging sophistication in computational resources available to attackers, demanding constant improvement in hash functions [78]. For example, notably, despite the usefulness of hash functions such as Message Digest Algorithm 5 (MD5) and Secure Hash Algorithm 2 family (SHA2), they were equally found to be prone to collision attacks whereby different values resulted to a similar hash value, defeating the aim of hash functions particularly as computational power grows [78]. The SHA family has come under criticism because of the collision resistance problem; they pose a loophole to attackers aiming at forging tokens or even compromising data integrity [81].

10.5 Hybrid Encryption

The use of both symmetric and asymmetric encryption is possible since each method has its merits that can be of great security importance to tokens in transit. Asymmetric encryption is used in the transfer of the symmetric key, which is used for the actual encryption of the token. This is a method of key exchange that has superior security advantages as the asymmetric key is used in exchanging keys, while the efficiency of symmetric encryption is used in encrypting the token. This is employed in most protocols like SSL/TLS (Secure Sockets Layer/Transport Layer Security).

This approach boosts security by applying symmetric encryption as Advanced Encryption Standard (AES) and key distribution features of asymmetric approaches like RSA or Elliptic Curve Cryptography (ECC) [82]. For example, hybrid systems can greatly minimize the problem of processing large data that is typically found in public-key cryptography. The use of more than one encryption algorithm is not only enhancing the security aspect but also the performance, thus making hybrid encryption the best choice for today's cryptographic requirements in token transmission [82].

In addition, one potential issue is the degree of security provided by both types of encryption; the security of both is fundamental to the encryption process, and if one is breached, then the other is affected as well [83]. The use of multiple encryption methods may lead to difficulty in managing the keys, especially due to the probability of key exposure [68].

Besides, in hybrid encryption, the trade-off between the encryption's performance characteristics can introduce a significant level of latency, which is considered a matter of importance in places that can require fast encryption [84]. Sometimes two or more algorithms are incorporated to form hybrid schemes, and if the integration is not perfect, it may not yield the anticipated results on security enhancements, which could introduce breaches into the system [85].

10.6 Zero-Knowledge Proofs (ZKP)

The Zero-knowledge proofs (ZKP) have been identified as a secure means of token exchange, especially in applications like e-commerce and other cryptographic applications. They are beneficial for a prover since they require no detailed information to prove the validity of the statement, and with this data alone, confidentiality is maintained without revealing the contents of the data during token transmission. This property is important, especially in online transactions where payments should always be secure; this has been evident with the use of ZKPs in protocols such as Zcash [86]. These approaches are particularly important in privacy-preserving systems, where the details of the transaction must remain private while the validity of the transaction has to be verified, like in digital signatures and authentication systems [35].

Even though, through its usage, it would be possible to prove the certainty of the information without revealing its content, Zero-Knowledge Proofs (ZKPs) are associated with a considerable computational burden, which results in performance degradation when applied in real-world use scenarios. For example, the computational overhead in constructing and verifying ZKPs reduces their applicability due to scalability issues, especially in a large number of transactions in environments such as e-commerce [86].

Due to poor implementations, the use of ZKPs in practical applications has been severely constrained in the past. This is because ZKPs normally entail the deployment of complex cryptographic structures that could also present extra vulnerability factors, especially where the foundational hypothesis has not been well built. Nevertheless, as it was mentioned above, ZKPs improve privacy, but it is crucial to underline that they do not presuppose the complete absence of information leakage, as several works indicate that decoy-based anonymity may disclose some relationships [87]. Despite the design of the ZKPs to enhance privacy, a side-channel attack may access information leakage in the process of the proof [88]. It is this vulnerability that can negatively impact the security assurances that ZKPs set out to deliver.

11 Analysis, Recommendations, and Works Done by Other Researchers

In this section, we explore some of the key recommendations and protocols developed by other researchers, highlighting their contributions to advancing knowledge and practices within the field. Their works provide invaluable insight into best practices and offer a foundation for future research.

11.1 Transport Layer Security (TLS)

The evolution of TLS, particularly the transition from TLS 1.2 to TLS 1.3, has introduced various enhancements, most notably in terms of speed, security, and the simplification of the handshake process [89]. TLS 1.3, standardized by the Internet Engineering Task Force (IETF) in 2018, eliminates outdated cryptographic algorithms and enforces stronger encryption methods, which significantly reduce the risk of various attack vectors present in earlier versions.

Bhat and Kavasseri highlight the application of TLS in securing communications within 5G networks for tele-surgery, emphasizing that any vulnerabilities in the authentication process can compromise patient safety and privacy. Their proposed enhancements, which include multi-factor and biometric authentication, build upon TLS's foundation to provide robust security for critical applications [90]. Similarly, in the context of cloud computing, multi-factor authentication integrated with TLS demonstrates a highly secure authentication process, establishing a secure communication channel while verifying user identity through multiple verification factors, including passwords and one-time passcodes [91].

Furthermore, the need for reliable transmission of data in Industrial Internet of Things (IIoT) settings, such as SCADA systems, is addressed in Yang et al.'s work. They propose utilizing TLS not only for encryption but also for trusted token authentication, thereby preventing potential security breaches due to physical attacks [92].

To reduce risks associated with Transport Layer Security, it is advised to strictly follow the secure TLS configuration guidelines alongside applying strong cipher techniques and updating the protocol from time to time [93]. Further, it is known that the use of Datagram Transport Layer Security (DTLS) in situations where real-time communication is needed can increase the level of security without negatively affecting the speed [94].

11.2 Inter-Blockchain Communication (IBC)

The security architecture employed in IBC must be robust enough to withstand potential vulnerabilities such as unauthorized access or data tampering during cross-chain transactions. To address these concerns, it is advisable to employ additional encryption layers during transmission processes, as proposed by Chen et al., where a hybrid encryption algorithm can fortify the authentication procedures for tokens transmitted between blockchains [68].

The complexity of managing trust among multiple participants in an inter-blockchain environment poses additional hurdles. Trust management frameworks that leverage consensus mechanisms can significantly enhance security. As highlighted by Ghaffari et al., incorporating smart contracts can aid in ensuring data integrity and confidentiality, thus allowing for trustless interactions across different blockchain networks [95]. Implementing federated models that utilize multiple validators may also enhance trust without relying on a single point of failure, as discussed by Kumar et al. in the context of the pharmaceutical supply chain [96].

Beyond enhancing security and trust, scalability also remains a pivotal concern for inter-blockchain communication. The integration of a scalable architecture that can handle a growing number of transactions across various networks is crucial. Strategies involving Decentralized Autonomous Organizations (DAOs) and the implementation of industry standards could facilitate smoother data exchanges and improve transaction throughput. For instance, the introduction of interledger protocols aimed at supporting industrial Internet of Things (IoT) applications demonstrates a practical model that addresses scalability challenges and enables cross-chain communication [97].

11.3 WebSocket

Research comparing WebSocket with protocols like HTTP, MQTT, and gRPC reveals that while WebSockets excel in scenarios requiring low latency and real-time bidirectional communication, they might not be optimal for every use case. For example, REST and GraphQL can be more suitable for applications with less stringent real-time requirements due to their simplicity and established caching mechanisms [98]. Despite its advantages, WebSocket communication is not without its vulnerabilities. One study highlighted various security attacks, including cross-site scripting (XSS) and denial-of-service (DoS) attacks, that specifically target WebSocket implementations [99].

The open nature of WebSocket connections also opens them to potential eavesdropping if not properly secured, necessitating robust authentication and encryption strategies. In real-time chat applications, WebSockets are utilized for instant message delivery, providing users with a seamless communication experience [100].

Similarly, in project management applications, WebSocket communication enables instant synchronization among stakeholders, ensuring users receive real-time updates on project status and task completion [101]. Moreover, developments such as real-time auction platforms demonstrate how WebSockets enhance user interaction by providing immediate bid updates [102].

11.4 Smart Contracts

Smart contracts share a degree of code on platforms such as Ethereum, which poses vulnerabilities because of the interlink since one contract can affect others [103]. Real-life scenarios like the decentralized autonomous organization hack, famously known as The DAO hack, show the importance of installing adequate measures since these vulnerabilities can cause severe monetary losses as it was in the case of the DAO hack where $60 million was lost as a result of reentrancy injection [104] Oyente and Mythril are some of the modern tools that help developers spot these problems [105]. Therefore, the problem of insecure token transmission can be solved by combining automated vulnerability detection systems or tools, secure coding, and rigorous testing of smart contracts.

11.5 The Interledger Protocol (ILP)

The Interledger Protocol (ILP) presents several challenges related to token transmission. First, it integrates multiple communication layers, which often requires additional transaction management. For example, notaries are typically needed to oversee transactions, creating potential points of failure. These intermediaries demand robust security measures to prevent unauthorized access. Therefore, there is a need to strengthen the security of ILP by incorporating strong cryptographic features and effective auditing processes. Enhancing the protection of secret-sharing protocols is also crucial to address these vulnerabilities and mitigate the associated risks [106].

11.6 Message Queuing Telemetry Transport (MQTT)

For IoT applications, the MQTT protocol is commonly used because of its low bandwidth consumption and being an efficient “publisher/subscriber” model. However, the security of this protocol is questionable, particularly in the secure transmission of tokens. A noteworthy issue is the denial of service (DoS) attacks on the communication between clients and brokers, which may lead to data loss or unavailability of services.

MQTT, as a protocol, does not have a security feature enshrined in it, and therefore, to enhance security during the transmission of data, one has to secure it externally by use of Transport Layer Security (TLS) or Secure Sockets Layer (SSL) [107]. To address these risks, the appropriate mechanism includes secure forms of authentication and strong encryption standards, coupled with comprehensive security audits to determine areas within the system with possible flaws and measures for it [108].

Furthermore, for cooperating healthcare smart devices, it is useful to incorporate Secure Transport Layers, for instance, MQTT over TLS, which contributes to data integrity and confidentiality in the course of token transmission [45]. It needs to be noted that the utilization of blockchain technology for access control may also provide a decentralized way to enhance security in connecting MQTT [109]. Their application through the layers of strong authentication, secure transport protocols, and advanced access control will improve MQTT token transmission security and subsequently provide more reliable token transmission systems.

11.7 Peer-To-Peer (P2P)

Research conducted by [110] emphasizes the importance of robust data management strategies within file-sharing systems to safeguard users' identities and data. Likewise, Chen et al. [111] propose a privacy-preserving protocol for federated learning in P2P networks, illustrating the ongoing need for enhanced data protection mechanisms within decentralized systems.

There is a need to implement secure communication frameworks within Peer-to-peer (P2P) networks. For instance, as adaptive mechanisms, Bayesian games can be used to enhance security in mobile P2P ecosystems and ensure trusted authorization of resources, thereby preventing malicious actors from penetrating and tampering with token transmission. Additionally, this involves reputation management systems that utilize decentralized identity verification to prevent malicious actors from entering the technology environment and interacting with peers, thereby maintaining participants' trust in token exchanges.

One common threat is the Sybil attack, in which an attacker registers multiple fake identities and can alter the normal functioning of a network, which may disrupt token exchange and endanger genuine transactions. Similar to conventional networks, P2P networks are prone to malware spread, where active worms penetrate the existing vulnerabilities on the network and increase the risks of token transfer tampering. The vulnerabilities with P2P network security should be solved using multiple approaches that include effective security measures and managing the reputation of token transmission [59].

12 Cryptographic Analysis Recommendations and Works Done by Other Researchers

Numerous researchers have contributed to the advancement of cryptographic analysis, introducing innovative methods for vulnerability detection, algorithmic efficiency, and secure key management. This section explores key recommendations in the field, highlighting significant contributions and the works of prominent researchers that have shaped the current state of cryptographic analysis.

12.1 Symmetric Encryption

Asymmetric encryption is the most adopted technique for securing token transmission since it is fast and efficient. studies have reported the development of secure key exchange methods that integrate new algorithms aimed at bolstering the stability and security of symmetric encryption against emerging quantum computing threats [112]. Furthermore, the design of methods specifically for the Internet of Things (IoT) has gained traction, emphasizing the need for both lightweight and efficient symmetric encryption solutions to protect sensitive data transmitted between IoT devices [113].

In the domain of mobile communications, particularly for NFC (Near Field Communication) applications, symmetric encryption protocols have been shown to provide robust authentication measures that enhance security. These protocols often implement additional security features, such as time-stamping and hash functions, to further improve the confidentiality and performance of the authentication process [114]. This multifaceted approach illustrates the versatility and adaptability of symmetric encryption techniques in various technological contexts.

As researchers continue to identify vulnerabilities within existing encryptions, recent studies have also highlighted the need for improved S-Box constructions within symmetric systems, proposing new methods derived from chaos theory [115]. These enhancements aim to bolster the security of symmetric algorithms against cryptographic attacks while maintaining high performance levels.

12.2 Asymmetric Encryption

In asymmetric encryption, one disadvantage is the low speed in data encryption and decryption as compared to symmetric encryption, this makes it difficult for bulk data transfer. Besides, these algorithms are vulnerable to attacks because of the slow processing of their computational capabilities while quantum computing can crack such computations with faster encryption time [116]. Han et al. developed an attribute-based encryption system for the Internet of Vehicles (IoV) that employs asymmetric encryption to ensure access control and data protection [117]. This demonstrates a shift towards specialized implementations of asymmetric methods tailored for specific applications, such as vehicular networks. Abdul and Arumugam proposed a hybrid encryption scheme that utilizes both symmetric and asymmetric encryption algorithms [118]. Their approach aims to balance security and efficiency, stating that the use of asymmetric encryption often comes with increased computational overhead.

Xu et al. introduced a lightweight mutual authentication and key agreement scheme that significantly reduces computational cost compared to traditional asymmetric encryption, particularly relevant for resource-constrained environments like the Internet of Things [119].

A significant drawback of asymmetric encryption is its computational intensity compared to symmetric methods. The overhead of using asymmetric keys for encryption and decryption processes can lead to performance bottlenecks, especially in environments requiring high throughput [120]. Despite providing enhanced security features, asymmetric encryption schemes are not immune to various attacks. For example, they can exhibit vulnerabilities to chosen-plaintext attacks, as noted in discussions regarding the limitations of complex encryption systems [121].

In applications requiring low latency, such as real-time communication frameworks, asymmetric encryption can introduce unacceptable delays. Jangid and Lin suggest that utilizing symmetric encryption can mitigate some of these performance concerns in connected vehicle systems by favorably opting for symmetrical keys over asymmetric ones [122].

Furthermore, improvements in cryptographical methods and adopting Quantitative risk analysis while incorporating other security features, increase the reliability of asymmetric encryption of tokens during transmission which is of paramount importance in defense against ever-evolving threats. For instance, homomorphic encryption techniques enable computations to be performed on encrypted data without necessarily decrypting them and thereby maintain the data confidentiality even when processing [123]. This can be adopted in token transmission as it has been applied in cases where integral data sharing is crucial, for instance, genomic data, which requires high levels of privacy [67].

12.3 Digital Signatures

Recent advancements in the field have explored novel digital signature schemes beyond conventional public key systems. For instance, quantum digital signatures (QDS) have emerged as a promising alternative, leveraging the principles of quantum mechanics to provide inherent security against potential quantum computing threats [124]. As outlined by Duan, the transition to quantum-resilient digital signatures is vital for future-proofing electronic communications, especially within sensitive domains like governmental and financial transactions [81]. Additionally, studies by Li et al. describe how newer hashing techniques can enhance the security landscape for digital signatures, allowing for improved integrity and authenticity in digital communications.

Exploration into alternative cryptographic foundations has also led to the evaluation of code-based and lattice-based digital signature schemes as candidates to replace traditional systems, which are susceptible to advancements in computational power [125,126]. Such schemes aim to maintain security and robustness while ensuring operational efficiency.

12.4 Hash Functions

Historically, older hash algorithms such as MD5 and SHA-1 have been found to exhibit vulnerabilities under modern attack strategies, underscoring the pressing need for more secure alternatives. Studies have observed that improvements in processing power and analysis techniques have rendered these previously robust hash functions increasingly susceptible to cryptanalysis [80]. This has catalyzed efforts to develop innovative cryptographic hash functions that maintain essential security requirements while addressing these evolving threats.

The Keccak hash function, known for its implementation as SHA-3, exemplifies an advanced cryptographic hash function capable of providing high throughput [127]. Its design not only enhances performance but also significantly strengthens security against various attacks. The avalanche effect—where a slight alteration in input leads to significant changes in the output—remains a central characteristic of cryptographic hash functions, ensuring that even minor modifications are detectable [128].

Advancements also include the utilization of chaotic systems in hash function design, which leverage complex mathematical frameworks to enhance security. For example, Liu et al. introduced a keyed hash function based on hyper-chaotic systems, which significantly augments the diffusion properties essential for secure hashing [129]. Similarly, research has shown that chaotic neural networks can produce robust hash functions, furthering the security of applications such as message authentication and digital signatures [130].

Moreover, the SHA family of algorithms continues to evolve, with analyses emphasizing their importance in maintaining the integrity and authenticity of digital communications. Khan et al. provide an overview of the evolution and analysis of this family, highlighting its role in data verification and integrity assurance across various applications, including cryptocurrency [131]. Despite the advancements, the potential for vulnerabilities in these widely used algorithms necessitates continual refinement and adaptation, as shown in more recent works focusing on optimizing implementations for application-specific contexts, such as FPGA platforms [132].

In the realm of image processing, perceptual hashing has gained traction, enabling robust integrity verification against alterations, a crucial feature in high-resolution remote sensing applications [133]. By employing specialized hashing methods tailored for images, this approach aligns well with the requirements for maintaining data integrity without compromising security. Differentiating hash functions by their underlying structures and performance can guide developers in selecting the most appropriate algorithms to reinforce cryptographic applications [134].

12.5 Hybrid Encryption

One of the significant implementations of hybrid encryption involves the integration of Advanced Encryption Standard (AES) and public key encryption methods like RSA or Elliptic Curve Cryptography (ECC). For instance, Yang et al. propose a hybrid architecture employing AES and RSA that enhances computational speed while maintaining security for IoT environments [135]. Additionally, Liu et al. demonstrate a hybrid encryption approach that combines symmetric encryption with attribute-based encryption (CP-ABE) to ensure both efficiency and access control over sensitive medical data [136]. Such collaborations are essential in fulfilling the dual requirements of strong encryption and practical management of access rights.

Furthermore, the use of hybrid encryption has proven beneficial in securing video data transmission. Han et al. introduced a method that employs both elliptic curve and advanced encryption standards, achieving dual-layer encryption that amplifies security and efficiency in video file encryption [137]. Similarly, Shafiq et al. developed a hybrid approach for efficient internet transmission of video data using Modified Advanced Encryption Standard (MAES) combined with ECC, which highlights the growing importance of hybrid systems in addressing specific data types such as video [138].

Moreover, hybrid schemes have been effectively utilized in cloud computing environments. For instance, the study by Akter et al. assesses the performance of AES, RSA and their hybrid variant, illustrating that hybrid approaches substantially enhance data security while optimizing time efficiency during encryption and decryption processes in cloud storage scenarios [139]. Furthermore, the practicality of hybrid encryption is captured in the work of Ghaly and Abdullah, who present a hybrid model that significantly secures transactions and communications in software-defined networking (SDN) applications [140].

Recent innovations also emphasize hybrid encryption's role in healthcare. Srivenkateswaran et al. propose a federated learning framework fortified with hybrid encryption, showcasing a modern application that addresses the intricate security needs within healthcare systems [141]. This is complemented by the work of Liu et al., who tackled the problem of access control in cloud storage for medical data through a combination of DES and CP-ABE, thus ensuring both data privacy and controlled access [136].

12.6 Zero-Knowledge Proofs

The examination of Zero-Knowledge Proofs (ZKPs) reveals their significance in enhancing security across various technological fields, particularly in ensuring identity verification without the risk of revealing sensitive information. The foundational concept of ZKPs was introduced in the late 1980s by distinguished cryptographers Goldwasser, Micali and Rackoff, establishing a framework that allows one party, the prover, to convince another party, the verifier, of the validity of a statement without disclosing any additional information about that statement [142].

Recent developments have highlighted the versatility of ZKPs in diverse applications, such as blockchain technology, e-commerce and secure device communication. For instance, the integration of ZKPs in blockchain technology allows for the construction of privacy-preserving transactions and secure smart contracts, as demonstrated in applications like Zcash, which uses ZKPs to ensure confidentiality during transactions [143]. The introduction of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) by Gennaro et al. exemplifies how ZKPs can provide short proofs for various computations, enhancing efficiency without compromising security [144].

In the context of the Internet of Things (IoT), ZKPs are increasingly employed to facilitate secure device-to-device communication without compromising user privacy. Their application allows devices to authenticate each other and verify identity claims without exposing sensitive attributes, addressing critical challenges in a landscape where numerous devices are interconnected [145]. Chai et al. assert that zero-knowledge authentication is foundational for IoT security, facilitating a method where devices can confirm their identity while keeping their credentials confidential [146].

Further innovations in the realm of ZKPs include explorations into non-interactive ZKPs, which simplify the process by reducing the need for back-and-forth communication between the prover and verifier, enhancing efficiency. Studies on specialized protocols, such as those based on elliptic curves, have underscored the performance advantages and heightened resistance to specific cryptographic attacks, making them suitable for a range of applications from secure login mechanisms to two-factor authentication systems [147].

Moreover, recent research underscores the potential of combining ZKPs with other encryption techniques, such as in the context of intelligent connected vehicles, where such integration safeguards the privacy of users while enabling secure data sharing [148]. Luo's work showcases the effectiveness of merging ZKPs with post-quantum cryptography, ensuring that systems remain secure against future quantum computing threats.

13 Conclusion

On balance, each method for transmitting tokens has shown some advantages and possible weaknesses in light of the above key security aspects. As technology advances within the digital environment, so does the importance of protecting the methods of tokens' transfer in terms of preserving information's integrity, authorship and confidentiality as well as overcoming new threats and challenges specific to the development of the technology.

The analysis of communication protocols and cryptographic techniques applied in secure token transmission reveals the intricate interplay between security and efficiency in modern systems. Various studies highlight the importance of tailored protocols that can adeptly handle the requirements of specific applications, such as telemedicine, IoT and decentralized networks.

The use of encryption techniques and robust authentication mechanisms is critical in ensuring the secure transmission of tokens across diverse communication platforms. The effective integration of communication protocols with sophisticated cryptographic techniques is indispensable for the secure transmission of authentication tokens. As the technological landscape continues to evolve, ongoing research must focus on refining these strategies to anticipate and mitigate emerging security threats while considering the practical limitations of implementation in real-world applications. Future studies should explore innovative solutions that balance security, usability and efficiency, particularly as the dynamics of cyber threats and user needs continue to develop.

The integration of quantum-resistant cryptographic techniques is paramount. Given the threats posed by quantum computing to traditional cryptographic algorithms, utilizing quantum tokens can significantly enhance security and ensure user privacy without necessitating the storage of quantum states. Recent advancements indicate that such implementations could provide instant validation and unforgeability, thus securing token transmission in scenarios prone to cyber threats [149]. Incorporating quantum key distribution methods alongside these tokens could further harden communication channels, particularly in critical sectors such as healthcare and finance [19].

Employing advanced Lightweight Elliptic Curve Cryptography (ECC) in combination with token-based authentication mechanisms has been shown to enhance the security of communication protocols in resource-constrained environments, such as Internet of Things (IoT) networks [150]. Future research should focus on optimizing ECC routines to support complex token authentications without overburdening the limited computational power of these devices. This approach could also serve as a universal solution across various use cases, from smart consumer products to industrial IoT applications.

It is crucial to address the increasing need for usability in secure token transmission systems. Current systems often favor stringent security protocols that complicate user experiences. Incorporating biometric authentication methods and multi-factor authentication (MFA) can improve security while simplifying access processes [151]. User-oriented designs that incorporate feedback mechanisms from these methods could lead to more widely accepted authentication systems.

Continuous research into the interoperability of different blockchain systems is necessary to facilitate seamless token exchanges across disparate networks. Enhancing inter-blockchain communication protocols can minimize delays and increase efficiency in token transactions, critical for applications requiring immediate security responses, such as finance or healthcare [25].

Trends in Token Transmission

One common trend is the application of Mult-Token for improving data authenticity and security to the structure of Content-Centric Networking (CCN). Youn et al. also propose a multiple-token approach known as LIVE which enables the publisher to control tokens for cached content through token control mechanisms and enhance both computation and communication efficiency even with the disadvantage of hash chain transmission errors [152]. This method aligns with the findings of Dash et al., who propose a MAC-cum-routing protocol that employs a robust token distribution technique to facilitate collision-free data transmission in wireless sensor networks (WSN), thereby optimizing energy consumption and throughput [153]. Token-based authentication mechanisms are gaining traction, particularly in micro-application architectures. Chen et al. elaborates on the use of symmetric and asymmetric encryption techniques for token encryption as well as some of the critical yet neglected aspects of token transmission [68]. Token passing techniques are quite helpful in maintaining secure communication as the complexity of network environments rises. The Multi-Channel Token Passing (MCTP) method for token passing is alluded for improving packet control efficiency, thus showing how token passing can resolve problems emanating from dynamic rate adjustments in multi-flow scenarios consequently, this method is more suitable for vehicular networks [24]. Cross-chain technologies are seen as a way of responding to the issue of blockchain interoperability, this is backed up by the Inter-Blockchain Communication (IBC) protocol, which allows safe and swift token and data transfer across different zones within the Cosmos network [25]. The trends evident in token transmission techniques suggest that efficiency, security and flexibility are becoming integrated into many applications. Multi-token systems, strong authentication methods, opportunistic routing and blockchain technologizes used in token transmission show that token transmission is an evolving process that can only improve the performance and security of future network architectures.

Acknowledgement: This work was done in affiliation with The Co-Operative University of Kenya. The institution provided professional academic mentorship and a conducive environment to conduct research.

Funding Statement: No funding was received to assist with the preparation of this manuscript. No funding was received for conducting this study. No funds, grants, or other monetary support were received.

Author Contributions: All authors contributed to the conception and design of the study. Michael Juma Ayuma, the first author, was responsible for the conceptualization, methodology, literature review, and drafting of the original manuscript. Shem Mbandu Angolo, Philemon Nthenge Kasyoka, and Simon Maina Karume, the second, third, and fourth authors, respectively, contributed to the conceptualization, review, and supervision of the study. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used in this study is publicly available on papers published in the relevant journals as recorded in this manuscript.

Ethics Approval: Not applicable.

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

Abbreviations

QDS	Quantum digital signatures
JSON	JavaScript Object Notation
MFA	Multi-factor authentication
CSRF ML	SHIELD: Cross-Site Request Forgery Machine Learning Shield
MP-HTLC	Multiparty hash time lock contracts
SSO	Single Sign On
OTP	One Time Password
PINs	Personal Identification Numbers
2FA	Two-factor authentication
IoT	Internet of Things
ECC	Elliptic curve cryptography
AES	Advanced Encryption Standard
DES	Data Encryption Standard
SSL	Secure Socket Layer
JWTs	JSON Web Tokens
DeFi	Decentralized Finance
NFTs	Non-fungible tokens
PUFs	Physically Unclonable Functions
XSS	Cross-site scripting
WSNs	Wireless Sensor Networks
MCTP	Multi-channel token passing
TLS	Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
HTLCs	Hashed Timelock Contracts
ILP	Interledger Protocol
MQTT	Message Queuing Telemetry Transport
MD5	Message Digest Algorithm 5
SHA2	Secure Hash Algorithm 2 family
SSL/TLS	Secure Sockets Layer/Transport Layer Security
ZKP	Zero-Knowledge Proofs
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
DTLS	Datagram Transport Layer Security
DAOs	Decentralized Autonomous Organizations
gRPC	Remote Procedure Call
CP	ABE: Ciphertext: Policy Attribute: Based Encryption
NFC	Near Field Communication
MAES	Modified Advanced Encryption Standard
SDN	Software-defined networking
CCN	Content Centric Networking
MCTP	Multi: Multi-Channel Token Passing

MITM	Man in the middle
IBC	Inter-Blockchain Communication
BFT	Byzantine Fault Tolerant
ODAP	Open Digital Asset Protocol
DoS	Denial of service
P2P	Peer-to-peer
TLS	Transport Layer Security
DeFi	Decentralized finance
HMAC	Message Authentication Codes

References

1. Singh A, Singh C. Security tools for Internet of Things: a review. Int Res J Adv Sci Hub. 2020;2(6):87–91. doi:10.47392/irjash.2020.42.
2. Dalimunthe S, Reza J, Marzuki A. Model for storing tokens in local storage (cookies) using JSON web token (JWT) with HMAC (hash-based message authentication code) in E-learning systems. J Appl Eng Technol Sci. 2022;3(2):149–55. doi:10.37385/jaets.v3i2.662.
3. Papaspirou V, Papathanasaki M, Maglaras L, Kantzavelou I, Douligeris C, Ferrag MA, et al. A novel authentication method that combines honeytokens and google authenticator. Information. 2023;14(7):386. doi:10.3390/info14070386.
4. Yalli JS, Hasan MH, Jung LT, Al-Selwi SM. Authentication schemes for Internet of Things (IoT) networks: a systematic review and security assessment. Internet Things. 2025;30(1):101469. doi:10.1016/j.iot.2024.101469.
5. Aldaoud M, Al-Abri D, Kausar F, Awadalla M. NDNOTA: ndn one-time authentication. Information. 2024;15(5):289. doi:10.3390/info15050289.
6. Lee B. Stateless one-time authenticated session resumption in TLS handshake using paired token. 2021. doi:10.20944/preprints202102.0102.v1.
7. Nyangaresi VO, Jasim HM, Mutlaq KA, Abduljabbar ZA, Ma J, Abduljaleel IQ, et al. A symmetric key and elliptic curve cryptography-based protocol for message encryption in unmanned aerial vehicles. Electronics. 2023;12(17):3688. doi:10.3390/electronics12173688.
8. Varalakshmi J, Dhanasekaran S. A dual hashing-based authentication and secure data transmission scheme for vehicular cloud environment using MECC with optimal resource allocation mechanism. Soft Comput. 2024;28(17):10423–37. doi:10.1007/s00500-024-09808-7.
9. MacKey TK, Miyachi K, Fung D, Qian S, Short J. Combating health care fraud and abuse: conceptualization and prototyping study of a blockchain antifraud framework. J Med Internet Res. 2020;22(9):e18623. doi:10.2196/18623.
10. Rechciński T. What else can AI see in a digital ECG? J Pers Med. 2023;13(7):1059. doi:10.3390/jpm13071059.
11. Al Manish Rana E. Enhancing data security: a comprehensive study on the efficacy of JSON web token (JWT) and HMAC SHA-256 algorithm for web application security. Int J Recent Innov Trends Comput Commun. 2023;11(9):4409–16. doi:10.17762/ijritcc.v11i9.9930.
12. Dietrich F, Louw L, Palm D. Blockchain-based traceability architecture for mapping object-related supply chain events. Sensors. 2023;23(3):1410. doi:10.3390/s23031410.
13. Pingos M, Christodoulou P, Andreou AS. Security and ownership in user-defined data meshes. Algorithms. 2024;17(4):169. doi:10.3390/a17040169.
14. Wan Muhamad Fokri EWNI. Classification of cryptocurrency: a review of the literature. Turk J Comput Math Educ. 2021;12(5):1353–60. doi:10.17762/turcomat.v12i5.2027.
15. Zilius K, Spiliotopoulos T, Van Moorsel A. A dataset of coordinated cryptocurrency-related social media campaigns. Proc Int AAAI Conf Web Soc Medium. 2023;17:1112–21. doi:10.1609/icwsm.v17i1.22219.
16. Schwiderowski J, Pedersen AB, Beck R. Crypto tokens and token systems. Inf Syst Front. 2024;26(1):319–32. doi:10.1007/s10796-023-10382-w.
17. Alekseenko AP. Legal regulation of the use of distributed ledger technologies in financial sector of Singapore. Rev Invest Univ Quindío. 2022;34(S2):381–91. doi:10.33975/riuq.vol34ns2.957.

18. Bellagarda J, Abu-Mahfouz AM. Connect2NFT: a web-based, blockchain enabled NFT application with the aim of reducing fraud and ensuring authenticated social, non-human verified digital identity. Mathematics. 2022;10(21):3934. doi:10.3390/math10213934.
19. Albshaier L, Almarri S, Hafizur Rahman M. A review of blockchain's role in E-commerce transactions: open challenges, and future research directions. Computers. 2024;13(1):27. doi:10.3390/computers13010027.
20. Yalli JS, Hilmi Hasan M, Tang Jung L, Ibrahim Yerima A, Adamu Aliyu D, Danjuma Maiwada U, et al. A systematic review for evaluating IoT security: a focus on authentication, protocols and enabling technologies. IEEE Internet Things J. 2025;12(12):18908–28. doi:10.1109/jiot.2025.3545737.
21. Vasquez-Cevallos L, Mitchell A, Muñoz-Hernández S, Herranz-Nieva Á, Garcia-Mingo A, De Corral-San Martin P, et al. Educational and clinical applications of a web- and Android-based telemedicine platform to expand rural health care in Ecuador. Telemed Rep. 2025;6(1):67–75. doi:10.1089/tmr.2024.0091.
22. Al-refai H, Alawneh A. User authentication and authorization framework in IoT protocols. 2022. doi:10.20944/preprints202208.0188.v1.
23. Oguta GC. Securing the virtual marketplace: navigating the landscape of security and privacy challenges in E-Commerce. GSC Adv Res Rev. 2024;18(1):84–117. doi:10.30574/gscarr.2024.18.1.0488.
24. Hsu CJ, Liu HI. Realizing opportunistic routing in multi-channel environments. IEEE Access. 2022;10:90655–68. doi:10.1109/access.2022.3200467.
25. Essaid M, Kim J, Ju H. Inter-blockchain communication message relay time measurement and analysis in *Cosmos*. Appl Sci. 2023;13(20):11135. doi:10.3390/app132011135.
26. Behera A, Sattath O, Shinar U. Noise-tolerant quantum tokens for MAC. arXiv:2105.05016. 2021.
27. Seo J. The future of digital authentication: blockchain-driven decentralized authentication in web 3.0. J Web Eng. 2024;23(5):611–36. doi:10.13052/jwe1540-9589.2351.
28. Ali Kazmi SH, Hassan R, Qamar F, Nisar K, Ibrahim AAA. Security concepts in emerging 6G communication: threats, countermeasures, authentication techniques and research directions. Symmetry. 2023;15(6):1147. doi:10.3390/sym15061147.
29. Kepkowski M, Hanzlik L, Wood I, Ali Kaafar M. How not to handle keys: timing attacks on FIDO authenticator privacy. Proc Priv Enhancing Technol. 2022;2022(4):705–26. doi:10.56553/popets-2022-0129.
30. Oren Y, Arad D. Toward usable and accessible two-factor authentication based on the piezo-gyro channel. IEEE Access. 2022;10:19551–7. doi:10.1109/access.2022.3150519.
31. Zhao D, Wang Z, Wei G, Alsaadi FE. l_2–l_∞ proportional–integral observer design for systems with mixed time-delays under round–robin protocol. Int J Robust Nonlinear Control. 2021;31(3):887–906. doi:10.1002/rnc.5328.
32. Bokolo AJ. Exploring interoperability of distributed ledger and decentralized technology adoption in virtual enterprises. Inf Syst E Bus Manag. 2022;20(4):685–718. doi:10.1007/s10257-022-00561-8.
33. Fett D, Hosseyni P, Kusters R. An extensive formal security analysis of the OpenID financial-grade API. In: 2019 IEEE Symposium on Security and Privacy (SP); 2019 May 19–23; San Francisco, CA, USA. p. 453–71. doi:10.1109/sp.2019.00067.
34. Suomalainen J, Julku J, Vehkaperä M, Posti H. Securing public safety communications on commercial and tactical 5G networks: a survey and future research directions. IEEE Open J Commun Soc. 2021;2:1590–615. doi:10.1109/ojcoms.2021.3093529.
35. Yang YS, Lee SH, Wang JM, Yang CS, Huang YM, Hou TW. Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token. Sensors. 2023;23(10):4970. doi:10.3390/s23104970.
36. Ukrop M, Kraus L, Matyas V. Will you trust this TLS certificate? Digit Threat. 2020;1(4):1–29. doi:10.1145/3419472.
37. Wang Y, Liu X, Mao W, Wang W. DCDroid: automated detection of SSL/TLS certificate verification vulnerabilities in Android apps. In: Proceedings of the ACM Turing Celebration Conference; 2019 May 17–19; Chengdu, China. doi:10.1145/3321408.3326665.
38. Zhang Z, Wang F, Liu Y, Lu Y, Liu X. CF-BFT: a dual-mode Byzantine fault-tolerant protocol based on node authentication. Comput Mater Contin. 2023;76(3):3113–29. doi:10.32604/cmc.2023.040600.

39. Pillai B, Biswas K, Muthukkumarasamy V. Cross-chain interoperability among blockchain-based systems using transactions. Knowl Eng Rev. 2020;35:e23. doi:10.1017/s0269888920000314.
40. Pedreira C, Belchior R, Matos M, Vasconcelos A. Securing cross-chain asset transfers on permissioned blockchains. 2022. doi:10.36227/techrxiv.19651248.v2.
41. Flood J, McCullagh A. Blockchain's future: can the decentralized blockchain community succeed in creating standards? Knowl Eng Rev. 2020;35:e2. doi:10.1017/s0269888920000016.
42. Ghani R, Kamal Z, Farhan A. Blockchain-based E-Government system using WebSocket protocol. Eng Technol J. 2024;42(4):421–9. doi:10.30684/etj.2024.146559.1689.
43. Sunardi S, Afif A, Noviyanto F. Real time monitoring and irrigation control using the websocket protocol. In: Proceedings of the International Conference of Science and Technology for the Internet of Things; 2018 Oct 19–20; Yogyakarta, Indonesia. doi:10.4108/eai.19-10-2018.2282548.
44. Alwazzeh M, Karaman S, Shamma MN. Man in the middle attacks against SSL/TLS: mitigation and defeat. J Cyber Secur Mobil. 2020;9(3):449–68. doi:10.13052/jcsm2245-1439.933.
45. Badii C, Bellini P, Difino A, Nesi P. Smart City IoT platform respecting GDPR privacy and security aspects. IEEE Access. 2020;8:23601–23. doi:10.1109/access.2020.2968741.
46. Rathee G, Kerrache CA, Calafate CT, Song H. A trusted mechanism against device reputation attacks in Web-of-Things applications. Trans Emerg Tel Tech. 2024;35(6):e5011. doi:10.1002/ett.5011.
47. Xu W, Sun J, Cardell-Oliver R, Mian A, Hong JB. A privacy-preserving framework using homomorphic encryption for smart metering systems. Sensors. 2023;23(10):4746. doi:10.3390/s23104746.
48. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the Internet of Things. IEEE Internet Things J. 2019;6(2):1594–605. doi:10.1109/jiot.2018.2847705.
49. Neisse R, Hernandez-Ramos JL, Matheu-Garcia SN, Baldini G, Skarmeta A, Siris V, et al. An interledger blockchain platform for cross-border management of cybersecurity information. IEEE Internet Comput. 2020;24(3):19–29. doi:10.1109/mic.2020.3002423.
50. Haugum T, Hoff B, Alsadi M, Li J. Security and privacy challenges in blockchain interoperability—a multivocal literature review. In: The International Conference on Evaluation and Assessment in Software Engineering 2022. Gothenburg, Sweden: ACM; 2022. p. 347–56. doi:10.1145/3530019.3531345.
51. Alkadi R, Alnuaimi N, Yeun CY, Shoufan A. Blockchain interoperability in unmanned aerial vehicles networks: state-of-the-art and open issues. IEEE Access. 2022;10:14463–79. doi:10.1109/access.2022.3145199.
52. Thayyib AR, Salamah I, Halimatussa'diyah RA. IoT based monitoring system using MQTT protocol on tortilla chips cutting machine. Sistemasi. 2023;12(3):973. doi:10.32520/stmsi.v12i3.3328.
53. Selvi M, Gayathri A, Svn SK, Kannan A. Energy efficient and secured MQTT protocol using IoT. Int J Innov Technol Explor Eng. 2020;9(4):11–4. doi:10.35940/ijitee.b6264.029420.
54. Munshi A. Improved MQTT secure transmission flags in smart homes. Sensors. 2022;22(6):2174. doi:10.3390/s22062174.
55. Alasmari R, Alhogail AA. Protecting smart-home IoT devices from MQTT attacks: an empirical study of ML-based IDS. IEEE Access. 2024;12:25993–6004. doi:10.1109/access.2024.3367113.
56. Dryja KM, Markovic M, Edwards P. Fl$_y$trap: a blockchain-based proxy for authorisation and audit of MQTT connections. In: 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS); 2021 Dec 6–9; Gandia, Spain. p. 1–8. doi:10.1109/iotsms53705.2021.9704968.
57. Fernández F, Zverev M, Garrido P, Juárez JR, Bilbao J, Agüero R. Even lower latency in IIoT: evaluation of QUIC in industrial IoT scenarios. Sensors. 2021;21(17):5737. doi:10.3390/s21175737.
58. Hsu TC. Designing a secure and scalable service agent for IoT transmission through blockchain and MQTT fusion. Appl Sci. 2024;14(7):2975. doi:10.3390/app14072975.
59. Zakhary V, Agrawal D, El Abbadi A. Atomic commitment across blockchains. Proc VLDB Endow. 2020;13(9):1319–31. doi:10.14778/3397230.3397231.
60. Sable NP, Rathod VU, Mahalle PN, Railkar PN. An efficient and reliable data transmission service using network coding algorithms in peer-to-peer network. Int J Recent Innov Trends Comput Commun. 2022;10(1s):144–54. doi:10.17762/ijritcc.v10i1s.5819.

61. Wang C, Ren Y, Wu Z. Multi-hop anonymous payment channel network based on onion routing. IET Blockchain. 2024;4(2):197–208. doi:10.1049/blc2.12065.

62. Tobiloba B, Kelvin L. Scalability and deployment challenges in MQTT push to talk for large. 2023. doi:10.31219/osf.io/nszp4.

63. Astuti NRDP, Setiawan DP, Hakika DC. Comparative study of elgamal and luc algorithm in cryptographic key generation. ASEAN Eng J. 2023;13(4):61–8. doi:10.11113/aej.v13.19184.

64. Dao MH, Beroulle V, Kieffer Y, Tran XT. How to develop ECC-based low cost RFID tags robust against side-channel attacks. In: Industrial networks and intelligent systems. Cham, Switzerland: Springer International Publishing; 2021. p. 433–47. doi:10.1007/978-3-030-77424-0_35.

65. Taş R, Tanrıöver ÖÖ. A manipulation prevention model for blockchain-based E-voting systems. Secur Commun Netw. 2021;2021(12):6673691. doi:10.1155/2021/6673691.

66. Adarbah HY, Moghadam MF, Maata RLR, Mohajerzadeh A, Al-Badi AH. Security challenges of selective forwarding attack and design a secure ECDH-based authentication protocol to improve RPL security. IEEE Access. 2023;11(3):11268–80. doi:10.1109/access.2022.3221434.

67. Cruz D, Almeida JR, Silva J, Oliveira JL. A reliable and secure method for sharing genomic data. In: Caring is sharing—exploiting the value in data for health and innovation. Vol. 302. Amsterdam, The Netherlands: iOS Press; 2023. p. 1071–2. doi:10.3233/shti230350.

68. Chen L, Chen M, Dai Z, Niu S. Micro-application security authentication based on key agreement hybrid encryption algorithm. In: Second International Symposium on Computer Applications and Information Systems (ISCAIS 2023); 2023 Mar 24–26; Chengdu, China. 18 p. doi:10.1117/12.2683350.

69. Agarwal S, Joshi G. Hybrid encryption of cloud processing with IOT devices using DNA and RSA cryptography. Int J Recent Innov Trends Comput Commun. 2023;11(6):21–7. doi:10.17762/ijritcc.v11i6.6767.

70. Manap AT, Abitova GA. Development of information technology for secure file storage based on hybrid cryptography methods. Bull Shakarim Univ Tech Sci. 2024;1(12):39–46. doi:10.53360/2788-7995-2023-4(12)-6.

71. Cultice T, Clark J, Yang W, Thapliyal H. A novel hierarchical security solution for controller-area-network-based 3D printing in a post-quantum world. Sensors. 2023;23(24):9886. doi:10.3390/s23249886.

72. Padmashree MG, Arunalatha JS, Venugopal KR. EBASKET ECC blended authentication and session key establishment technique for IoT. Int J Innov Technol Explor Eng. 2021;10(11):20–8. doi:10.35940/ijitee.k9461.09101121.

73. Thoi NT. Research and application of digital signatures in e-commerce today. J Contemp Issues Bus Gov. 2021;27(2):2276–81. doi:10.47750/cibg.2021.27.02.237.

74. Barbàra F, Schifanella C. MP-HTLC: enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract. Concur Comput. 2023;35(9):e7656. doi:10.1002/cpe.7656.

75. Wali A, Ravichandran H, Das S. A 2D cryptographic hash function incorporating homomorphic encryption for secure digital signatures. Adv Mater. 2024;36(23):e2400661. doi:10.1002/adma.202400661.

76. Gan L, Yokubov B. A performance comparison of post-quantum algorithms in blockchain. J Br Blockchain Assoc. 2023;6(1):1–10. doi:10.31585/jbba-6-1-(1)2023.

77. Mehibel N, Hamadouche M. Authenticated secret session key using elliptic curve digital signature algorithm. Secur Priv. 2021;4(2):e148. doi:10.1002/spy2.148.

78. Meng L, Chen L. Reviewing the ISO/IEC standard for timestamping services. IEEE Comm Stand Mag. 2021;5(3):20–5. doi:10.1109/mcomstd.011.2000083.

79. Ko H, Oh J, Kim SU. Digital content management using non-fungible tokens and the interplanetary file system. Appl Sci. 2024;14(1):315. doi:10.3390/app14010315.

80. Eldin SMS, El-Latif AAA, Chelloug SA, Ahmad M, Eldeeb AH, Diab TO, et al. Design and analysis of new version of cryptographic hash function based on improved chaotic maps with induced DNA sequences. IEEE Access. 2023;11:101694–709. doi:10.1109/access.2023.3298545.

81. Duan J, Li M, Ian H. A quantum algorithm for finding collision-inducing disturbance vectors in SHA-1. Phys Scr. 2023;98(11):115106. doi:10.1088/1402-4896/acfc79.

82. Janshi Lakshmi K, Sreenivasulu G. A compact hardware design and implementation on FPGA based hybrid of AES and keccak SHA3-512 for enhancing data security. Int J Electr Electron Res. 2024;12(1):195–202. doi:10.37391/ijeer.120128.
83. Jurcut A, Niculcea T, Ranaweera P, Le-Khac NA. Security considerations for Internet of Things: a survey. SN Comput Sci. 2020;1(4):193. doi:10.1007/s42979-020-00201-3.
84. Cha SM, Sasilatha T. Hardware implementation of hybrid model encryption algorithm for secure transmission of medical images. Int J Eng Adv Technol. 2019;9(1s):164–7. doi:10.35940/ijeat.a1042.1091s19.
85. Kuppuswamy P, Al Khalidi Al-Maliki SQY, John R, Haseebuddin M, Ali Shaik Meeran A. A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. Bull Electr Eng Inform. 2023;12(2):1148–58. doi:10.11591/eei.v12i2.4967.
86. Tangka GMW, Delviolin EO, Chou HM. Zero-knowledge proof application in ecommerce payment. Taiwanproceeding. 2022;4:69–75. doi:10.52162/4.2022162.
87. Herskind L, Katsikouli P, Dragoni N. Privacy and cryptocurrencies—a systematic literature review. IEEE Access. 2020;8:54044–59. doi:10.1109/access.2020.2980950.
88. Perera MNS, Koshiba T. Almost fully secured lattice-based group signatures with verifier-local revocation. Cryptography. 2020;4(4):33. doi:10.3390/cryptography4040033.
89. Arfaoui G, Bultel X, Fouque PA, Nedelcu A, Onete C. The privacy of the TLS 1.3 protocol. Proc Priv Enhancing Technol. 2019;2019(4):190–210. doi:10.2478/popets-2019-0065.
90. Bhat S, Kavasseri A. Enhancing security for robot-assisted surgery through advanced authentication mechanisms over 5G networks. Eur J Eng Technol Res. 2023;8(4):1–4. doi:10.24018/ejeng.2023.8.4.3064.
91. Okeke RO, Orimadike SO. Enhanced cloud computing security using application-based multi-factor authentication (MFA) for communication systems. Eur J Electr Eng Comput Sci. 2024;8(2):1–8. doi:10.24018/ejece.2024.8.2.593.
92. Yang YS, Lee SH, Chen WC, Yang CS, Huang YM, Hou TW. TTAS: trusted token authentication service of securing SCADA network in energy management system for industrial Internet of Things. Sensors. 2021;21(8):2685. doi:10.3390/s21082685.
93. Carelli A, Palmieri A, Vilei A, Castanier F, Vesco A. Enabling secure data exchange through the IOTA tangle for IoT constrained devices. Sensors. 2022;22(4):1384. doi:10.3390/s22041384.
94. Friesen M, Karthikeyan G, Heiss S, Wisniewski L, Trsek H. A comparative evaluation of security mechanisms in DDS, TLS and DTLS. In: Kommunikation und bildverarbeitung in der automation. Berlin/Heidelberg, Germany: Springer; 2020. p. 201–16. doi:10.1007/978-3-662-59895-5_15.
95. Ghaffari F, Bertin E, Hatin J, Crespi N. Authentication and access control based on distributed ledger technology: a survey. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS); 2020 Sep 28–30; Paris, France. p. 79–86. doi:10.1109/brains49436.2020.9223297.
96. Kumar M, Kumar L, Jai J, Sharma Y. MedBust: blockchain in pharmaceutical supply chain. Int J Sci Res Eng Manag. 2023;7(1):1–7. doi:10.55041/ijsrem17562.
97. Nikander P, Autiosalo J, Paavolainen S. Interledger for the industrial Internet of Things. In: 2019 IEEE 17th International Conference on Industrial Informatics (INDIN); 2019 Jul 22–25; Helsinki, Finland. p. 908–15. doi:10.1109/indin41052.2019.8972167.
98. Mironov DS. Research of API architecture for clientserver communication. Connectivity. 2024;167(1). doi:10.31673/2412-9070.2024.012629.
99. Kela R, Chawla A, Gaur P, Dr Manikandan K. Implementation of cyber security attacks and strategic mitigation mechanisms. Int J Adv Res Comput Sci. 2022;13(4):28–34. doi:10.26483/ijarcs.v13i4.6890.
100. Bhatikare P, Gavade S, Karande S, Bansode P, Garkal A. Real time chat application. Int J Innov Res Comput Commun Eng. 2025;13(2):1111–4. doi:10.31224/4468.
101. Pavan Kumar Reddy A. Dashboard real-time monitoring of construction projects. Int J Sci Res Eng Manag. 2025;9(5):1–9. doi:10.55041/ijsrem47451.
102. Tongase O. Developing AuctoLive: a real-time web-based auction and bidding platform. Int Sci J Eng Manag. 2025;4(6):1–9. doi:10.55041/isjem03980.

103. Lyu Q, Ma C, Shen Y, Jiao S, Sun Y, Hu L. Analyzing ethereum smart contract vulnerabilities at scale based on Inter-contract dependency. Comput Model Eng Sci. 2023;135(2):1625–47. doi:10.32604/cmes.2022.021562.

104. Hu T, Li J, Li B, Storhaug A. Why smart contracts reported as vulnerable were not exploited? IEEE Trans Dependable Secur Comput. 2025;22(3):2579–96. doi:10.1109/tdsc.2024.3520554.

105. Rodler M, Li W, Karame GO, Davi L. Sereum: protecting existing smart contracts against re-entrancy attacks. In: Proceedings 2019 Network and Distributed System Security Symposium; 2019 Feb 24–27; San Diego, CA, USA. p. 1–15. doi:10.14722/ndss.2019.23413.

106. Lagutin D, Kortesniemi Y, Siris VA, Fotiu N, Polyzos GC, Wu L. Leveraging interledger technologies in IoT security risk management. In: Security risk management for the Internet of Things: technologies and techniques for IoT security, privacy and data protection. Norwell, MA, USA: Now Publishers; 2020. p. 229–46. doi:10.1561/9781680836837.ch14.

107. Chark See Y, Xiang Ho E. IoT-based fire safety system using MQTT communication protocol. Int J Integr Eng. 2020;12(6):207–15. doi:10.30880/ijie.2020.12.06.024.

108. Azzedin F, Alhazmi T. Secure data distribution architecture in IoT using MQTT. Appl Sci. 2023;13(4):2515. doi:10.3390/app13042515.

109. Chen R, Du X, Hu J, Song T. Blockchain-based MQTT communication access control scheme for the Internet of Things. In: Second International Conference on Electronic Information Technology (EIT 2023); 2023 Mar 31–Apr 2. Wuhan, China. 159 p. doi:10.1117/12.2685781.

110. Hafeez KA. Building secure and legal file sharing system using JXTA platform [master's thesis]. Toronto, ON, Canada: Ryerson University; 2021.

111. Chen Q, Wang Z, Zhang W, Lin X. PPT: a privacy-preserving global model training protocol for federated learning in P2P networks. arXiv:2105.14408. 2021.

112. Jin J, Kim K. 3D CUBE algorithm for the key generation method: applying deep neural network learning-based. IEEE Access. 2020;8:33689–702. doi:10.1109/access.2020.2973695.

113. Jin H, Wang M, Wang L, Yang Q, Li Y, Long X, et al. The research focuses on the symmetric encryption scheme for industrial data based on MQTT. In: Third International Conference on Signal Processing and Communication Security (ICSPCS 2024); 2024 Jun 7–9; Chengdu, China. 1322209 p. doi:10.1117/12.3038673.

114. Lu HJ, Liu D. An improved NFC device authentication protocol. PLoS One. 2021;16(8):e0256367. doi:10.1371/journal.pone.0256367.

115. Aydın Y, Özkaynak F. Logistic and circle maps for robust S-box construction in cryptography. In: 2nd International Conference on Frontiersin Academic Research; 2023 Dec 4–5; Konya, Turkey. p. 274–8. doi:10.59287/as-proceedings.477.

116. Tang W, Gao Y. Application solutions of highway freight information systems based on quantum communication. Sci Rep. 2024;14(1):2668. doi:10.21203/rs.3.rs-3432631/v1.

117. Han M, Zhu M, Cheng P, Yin Z, Qu H. Implementing an efficient secure attribute-based encryption system for IoV using association rules. Symmetry. 2021;13(7):1177. doi:10.3390/sym13071177.

118. Abdul RF, Arumugam S. A novel data transmission model using hybrid encryption scheme for preserving data integrity. Adv Technol Innov. 2025;10(1):15–28. doi:10.46604/aiti.2024.14114.

119. Xu Z, Xu C, Liang W, Xu J, Chen H. A lightweight mutual authentication and key agreement scheme for medical Internet of Things. IEEE Access. 2019;7:53922–31. doi:10.1109/access.2019.2912870.

120. Awadh WA, Alasady AS, Hashim MS. A multilayer model to enhance data security in cloud computing. Indones J Electr Eng Comput Sci. 2023;32(2):1105. doi:10.11591/ijeecs.v32.i2.pp1105-1114.

121. Shi Y, Jiang D, Tsafack N, Ahmad M, Zhu L, Zheng M. Privacy data protection scheme using memristive hyperchaos and multi-scale block compressive sensing. Phys Scr. 2023;98(9):095206. doi:10.1088/1402-4896/ace93a.

122. Jangid MK, Lin Z. Towards a TEE-based V2V protocol for connected and autonomous vehicles. In: Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022; 2022 Apr 24; San Diego, CA, USA. p. 1–8. doi:10.14722/autosec.2022.23044.

123. Peng S, Cai Z, Liu W, Wang W, Li G, Sun Y, et al. Blockchain data secure transmission method based on homomorphic encryption. Comput Intell Neurosci. 2022;2022(1):3406228. doi:10.1155/2022/3406228.

124. Xia X, Hou T, Liu X, Zong C, Mu S. Protecting check-In data privacy in blockchain transactions with preserving high trajectory pattern utility. Wirel Commun Mob Comput. 2022;2022(4):9358531. doi:10.1155/2022/9358531.

125. Haidary Makoui F, Gulliver TA, Dakhilalian M. A new code-based digital signature based on the McEliece cryptosystem. IET Commun. 2023;17(10):1199–207. doi:10.1049/cmu2.12607.

126. Liu F, Zheng Z, Gong Z, Tian K, Zhang Y, Hu Z, et al. A survey on lattice-based digital signature. Cybersecurity. 2024;7(1):7. doi:10.1186/s42400-023-00198-1.

127. Sideris A, Sanida T, Dasygenis M. High throughput implementation of the keccak hash function using the nios-II processor. Technologies. 2020;8(1):15. doi:10.3390/technologies8010015.

128. Upadhyay D, Gaikwad N, Zaman M, Sampalli S. Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications. IEEE Access. 2022;10(6):112472–86. doi:10.1109/access.2022.3215778.

129. Liu H, Kadir A, Liu J. Keyed hash function using hyper chaotic system with time-varying parameters perturbation. IEEE Access. 2019;7:37211–9. doi:10.1109/access.2019.2896661.

130. Belal MM, Maitra T, Giri D, Das AK. Chaotic neural networks and farfalle construction based parallel keyed secure hash function. Secur Priv. 2022;5(6):e259. doi:10.1002/spy2.259.

131. Khan BUI, Olanrewaju RF, Morshidi MA, Mir RN, Mat Kiah MLB, Khan AM. Evolution and analysis of secured hash algorithm (Sha) family. Malays J Comput Sci. 2022;35(3):179–200. doi:10.22452/mjcs.vol35no3.1.

132. Devaji JP, Iyer NC, Mattimani R. Performance analysis of secure hash algorithm-2 (SHA-) and implementing on FPGA. In: ICT with intelligent applications. Singapore: Springer Singapore; 2021. p. 1–8. doi:10.1007/978-981-16-4177-0_1.

133. Ding K, Meng F, Liu Y, Xu N, Chen W. Perceptual hashing based forensics scheme for the integrity authentication of high resolution remote sensing image. Information. 2018;9(9):229. doi:10.3390/info9090229.

134. Zniti A, Ouazzani NE. Hash algorithm comparison through a PIC32 microcontroller. Bull Electr Eng Inform. 2023;12(4):2457–63. doi:10.11591/beei.v12i4.4982.

135. Yang S, Shao L, Huang J, Zou W. Design and implementation of low-power IoT RISC-V processor with hybrid encryption accelerator. Electronics. 2023;12(20):4222. doi:10.3390/electronics12204222.

136. Liu G, Guo F, Wu CK. Medical data sharing scheme based on hybrid encryption with revocable attribute. In: Fifth International Conference on Computer Information Science and Artificial Intelligence (CISAI 2022); 2022 Sep 16–18; Chongqing, China; 2023. 1256618 p. doi:10.1117/12.2667309.

137. Han Q, Wang L, Lee Y, Qin J. Video encryption scheme using hybrid encryption technology. Int J Internet Protoc Technol. 2020;13(1):1. doi:10.1504/ijipt.2020.105046.

138. Shafiq S, Latif S, Ibrahim J, Ilyas MSB, Imran A, Kryvinska N, et al. Optimizing video data security: a hybrid *MAES*-ECC encryption technique for efficient Internet transmission. PLoS One. 2024;19(11):e0311765. doi:10.1371/journal.pone.0311765.

139. Akter R, Khan MAR, Rahman F, Soheli SJ, Suha NJ. RSA and AES based hybrid encryption technique for enhancing data security in cloud computing. Int J Comput Appl Math Comput Sci. 2023;3:60–71. doi:10.37394/232028.2023.3.8.

140. Ghaly S, Abdullah MZ. Design and implementation of a secured SDN system based on hybrid encrypted algorithms. Telecommun Comput Electron Control. 2021;19(4):1118. doi:10.12928/telkomnika.v19i4.18721.

141. Srivenkateswaran C, Jaya Mabel Rani A, Senthil Kumaran R, Vinston Raja R. Securing healthcare data: a federated learning framework with hybrid encryption in cluster environments. Technol Health Care. 2025;33(3):1232–57. doi:10.1177/09287329241291397.

142. Yue M. Examining Schnorrs protocol in the context of zero-knowledge proofs. Theor Nat Sci. 2023;14(1):27–32. doi:10.54254/2753-8818/14/20240870.

143. Guo K, Ren H, Wang P. Research and application analysis of key technologies of zero-knowledge proof under the background of blockchain. Trans Comput Sci Intell Syst Res. 2024;5:94–7. doi:10.62051/sgykaq92.

144. Gennaro R, Minelli M, Nitulescu A, Orrù M. Lattice-based Zk-SNARKs from square span programs. In: CCS ’18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct 15–19; Toronto, ON, Canada. p. 556–73. doi:10.1145/3243734.3243845.

145. Zhang B, Zhang T, Xi Z, Chen P, Wei J, Liu Y. Secure device-to-device communication in IoT: fuzzy identity from wireless channel state information for identity-based encryption. Electronics. 2024;13(5):984. doi:10.3390/electronics13050984.

146. Chai Y, Liang R, Samtani S, Zhu H, Wang M, Liu Y, et al. Additive feature attribution explainable methods to craft adversarial attacks for text classification and text regression. IEEE Trans Knowl Data Eng. 2023;35(12):12400–14. doi:10.1109/TKDE.2023.3270581.

147. Strelkovskaya I, Onatskiy O, Yona L. Two-factor authentication protocol in access control systems. Inf Telecommun Sci. 2023;2023(2):17–25. doi:10.20535/2411-2976.22023.17-25.

148. Luo Y. Intelligent connected vehicle data security based on blockchain combining zero-knowledge proof and post-quantum cryptography. In: Second International Conference on Big Data, Computational Intelligence, and Applications (BDCIA 2024); 2024 Nov 15–17; Huanggang, China. 135500A p. doi:10.1117/12.3058773.

149. Pitalúa-García D, Kent A, Lowndes D, Rarity JG. Practical quantum tokens without quantum memories and experimental tests. In: Quantum Technology: Driving Commercialisation of an Enabling Science II; 2021 Sep 28–Oct 1; Glasgow, UK. 118810C p. doi:10.1117/12.2599038.

150. Sasirega L, Shanthi C. Lightweight ECC and token based authentication mechanism for WSN-IoT. Naučno-teh Vestn Inf Tehnol Meh Opt. 2022;22(2):332–8. doi:10.17586/2226-1494-2022-22-2-332-338.

151. Sen PL. Digital creativity and ethical challenges: the case of IoT in creative industries. J Digit Realism Mastery. 2023;2(2):66–71. doi:10.56982/dream.v2i02.113.

152. Youn TY, Kim J, Mohaisen D, Seo SC. Faster data forwarding in content-centric network via overlaid packet authentication architecture. Sustainability. 2020;12(20):8746. doi:10.3390/su12208746.

153. Dash S, Kumar S, Lenka MR, Swain AR. Multi-token based MAC-cum-routing protocol for WSN: a distributed approach. J Commun Softw Syst. 2019;15(3). doi:10.24138/jcomss.v15i3.709.