https://doi.org/10.70844/ijas.2025.1.17

Innovative Journal of Applied Science

Review Article

IJAS-25-050

A Comparative Analysis of SSL/TLS and Blockchain-Based Approaches Web-based Transactions

Zaki Rangwala*, Stefan Neskovic, Amirhossein Kompanizare

Department of Science, Wilfrid Laurier University, Waterloo, Canada

Corresponding Author: Zaki Rangwala, Department of Science, Wilfrid Laurier University, Waterloo, Canada, E-mail: rang6860@mylaurier.ca

Received date: 22 January, 2025, **Accepted date:** 10 February, 2025, **Published date:** 17 February, 2025

Citation: Rangwala Z, Neskovic S, Kompanizare A (2025) A Comparative Analysis of SSL/TLS and Blockchain-Based Approaches Web-based Transactions. Innov J Appl Sci 2(1): 17.

Abstract

This study examines how well SSL/TLS and blockchain work to secure online transactions, especially purchase orders. Reviewing literature from 2013 to 2024 shows each method's key themes, benefits, and weaknesses. SSL/TLS is known for its strong encryption and solid framework but often has issues like centralization and threats from different attacks, leading to transaction delays and bottlenecks. On the other hand, blockchain technology uses decentralized protocols and features such as zero-knowledge proofs, promising better scalability and security, allowing for smooth and safe transactions without traditional middlemen. This comparison clarifies how effective each method is. It highlights the rise of blockchain as a viable option to the limits of SSL/TLS, deserving more study in e-commerce security.

Keywords: Computing and processing, Blockchain, Consensus mechanisms, Cryptographic protocols, Ecommerce, Immutable ledgers, Layer 2 scaling solutions, Mitm attacks, Public key infrastructure, SSL, TLS, Web security, Zero-knowledge proofs

Introduction

The current state of online transactions needs strong security measures to safeguard sensitive information from risks like Man-in-the-Middle (MITM) attacks. SSL/TLS has been crucial for internet security, using public key cryptography for safe data exchange. However, as online shopping grows, the drawbacks of SSL/TLS, such as its centralized structure and possible slowdowns, are becoming more evident. In contrast, blockchain technology offers a new way forward with its decentralized setup, using tools like zero-knowledge proofs to boost privacy and security. This analysis aims to highlight the pros and cons of both methods, especially in securing purchase orders on online shopping sites. By examining their effectiveness, scalability, and performance, this project aims to show the potential of blockchain in addressing the issues that SSL/TLS currently faces, leading to more robust transaction systems [1,2].

Literature Review

Background

The advancement of secure web-based transactions has prompted a closer examination of cryptographic protocols like SSL/TLS and blockchain technology. SSL/TLS employs asymmetric cryptography methods, prominently featuring the RSA algorithm, to establish secure connections through a handshake protocol. This handshake is not merely a technical formality; it involves the exchange of cryptographic keys designed to create a secure session, reducing the risk posed by threats. While this process is intended to uphold both data integrity and confidentiality, it is essential to critically consider the implications of its reliance on centralized certificate authorities. Such reliance can inadvertently create vulnerabilities, exposing the system to breaches and compromising user trust and safety (Figure 1).

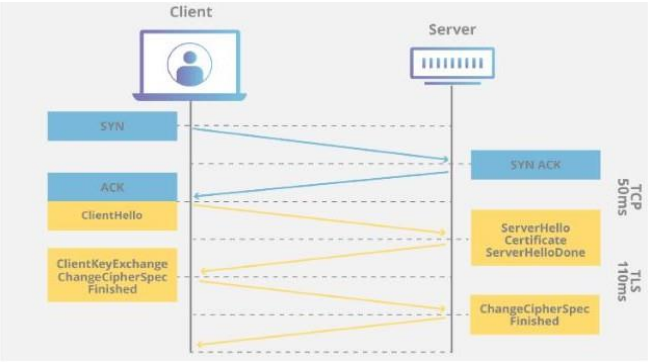

Figure 1: TLS Handshake with RSA Key Exchange.

In contrast, blockchain technology adopts a decentralized framework, utilizing consensus mechanisms like proof of work or proof of stake to authenticate transactions. This decentralized nature raises important questions about trust and governance in digital environments. Moreover, blockchain leverages zero-knowledge proofs to enhance privacy by enabling verification of transaction validity without revealing sensitive information. This method effectively safeguards against unauthorized access to transaction data while maintaining overall system integrity. The blockchain's

https://doi.org/10.70844/ijas.2025.1.17

Innovative Journal of Applied Science

architecture, characterized by immutable ledgers, promotes transparency and traceability, thus minimizing the need for intermediaries a point worth scrutinizing regarding the impact on transaction speed and efficiency. As indicated in the emergence of self-sovereign identity frameworks aligns well with these developments, advocating for user autonomy over personal data an imperative that SSL/TLS does not fully satisfy [3]. Ultimately, the convergence of these technologies underlines the pressing necessity for a hybrid model that systematically addresses the shortcomings of each approach in securing e-commerce transactions, particularly in the context of increasing demands for enhanced security and scalability in online environments.

Scope and Limitations

In the rapidly evolving web security landscape, comparing the scope and limitations of SSL/TLS and blockchain technology reveals critical insights. SSL/TLS protocols, while effective in securing data transit through encryption and authentication via Certificate Authorities, remain prone to vulnerabilities such as Man-in-the-Middle (MITM) attacks, which can undermine user trust [4]. Conversely, blockchain introduces decentralization and immutability, significantly enhancing the integrity of transactions by distributing data across a network of nodes, which reduces reliance on centralized authorities. For instance, research underscores the necessity of maintaining security in decentralized systems, an area where blockchain excels [5]. However, the scalability issues inherent to blockchain technology can hinder its effectiveness in high-transaction environments, a point supported by the insights derived from the comparative analysis [6]. Ultimately, while SSL/TLS provides immediate solutions for secure data transmission, blockchain's long-term benefits might address the growing security demands of e-commerce. Nonetheless, the practical implementation of blockchain still needs to be challenged by its relatively complex mechanisms and the need for broader adoption across existing infrastructures (Figure 2).

Approach	Security Level	Performance Impact	Scalability	Key Features	Usage
SSL/TLS	High	Low	Moderate	Encryption, Authentication, Integrity	Widely used for secure web communications
Blockchain	Very High	Moderate to High	Variable	Decentralization, Immutability, Transparency	Growing adoption in finance, supply chain, and other sectors

Figure 2: Comparative analysis of blockchain *vs* SSL/TLS approaches.

Discussion

Current debates about the security of online transactions highlight the critical distinctions between SSL/TLS and blockchain technologies. Although SSL/TLS protocols are essential for ensuring secure online communication, they exhibit significant weaknesses due to their centralized design and dependence on Certificate Authorities, which can become vulnerable points susceptible to Man-in-the-Middle (MITM) attacks [7]. On the other hand, blockchain technology offers a decentralized model that significantly improves security and trust, utilizing cryptographic methods such as zero-knowledge proofs to guarantee data integrity without revealing sensitive information. This built-in resilience is essential in light of the growing cyber threats aimed at e-commerce platforms [8]. By leveraging consensus mechanisms and unchangeable transaction records, blockchain solutions not only enhance security but also seek to tackle scalability challenges that have historically plagued conventional SSL/TLS protocols. Therefore, considering a hybrid architecture that combines SSL with blockchain, optimizing consensus algorithms for better feasibility, and exploring the potential of layer three solutions for scalability represent promising recommendations for overcoming the limitations of both protocols and achieving more secure and efficient web-based transactions in the future.

Utilizing a systematic review approach enabled this research to rigorously investigate the comparative frameworks of SSL/TLS and blockchain technologies in securing web-based transactions. The research question guiding this analysis aimed to explore these two methodologies' security, scalability, and performance attributes. An exhaustive search disclosed a wealth of literature from databases such as IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect, with carefully selected keywords, including "SSL/TLS security" and "blockchain e-commerce security." Inclusion criteria were strictly defined to encompass only peer-reviewed papers published between 2013 and 2024 that addressed the central research question, ensuring high-quality and relevant contributions to the discourse. Notably, studies that were not in English or did not pertain directly to SSL/TLS or blockchain in the context of e-commerce were methodically excluded, affirming the focus on impactful scholarly work [9]. This meticulous methodology enhances the credibility of the findings and paves the way for actionable insights into improving web-based transaction security through both protocols.

Comparative analysis of security mechanisms

The security landscape for web-based transactions has evolved significantly, revealing distinct advantages and challenges between SSL/TLS and blockchain systems. SSL/TLS protocols, while widely adopted, often face saturation from centralized certificate authorities, leading to vulnerabilities such as Man-in-the-Middle (MITM) attacks, which can compromise data integrity and privacy [10]. Conversely, blockchain technology addresses these shortcomings through decentralized mechanisms, reinforcing transaction security with its immutable ledger structure and consensus algorithms. These attributes enhance security and offer scalability benefits that SSL/TLS needs help to achieve under heavy transaction loads. Recent studies indicate that blockchain's unique features, such as smart contracts and zero-knowledge proofs, can further bolster security measures for e-commerce transactions [3]. A comparative analysis thus indicates that while SSL/TLS remains a vital component of online security, blockchain's innovative approach could mitigate many of its limitations, mainly as e-commerce transactions grow in complexity and volume (Figure 3).

Mechanism	Data Breaches	Encryption Strength (bit)	Average Response Time (ms)	Adoption Rate (%)
SSL/TLS	10	256	50	98
Blockchain	4	256	200	45
SSL/TLS Over Time	5	128	30	95
Blockchain Over Time	2	256	400	30

Figure 3: Security mechanisms comparison.

https://doi.org/10.70844/ijas.2025.1.17

Innovative Journal of Applied Science

Security features

In the evolving digital security landscape, the mechanisms supporting blockchain technology provide significant advantages that address shortcomings associated with traditional protocols like SSL/TLS. Unlike SSL/TLS, which relies on a centralized Certificate Authority (CA) to validate identities through the Handshake Protocol, blockchain utilizes decentralization and immutable blocks to enhance security. This allows for peer-to-peer interactions without intermediaries, reducing points of failure and vulnerabilities to attacks such as Man-in-the-Middle (MITM) threats [9]. Layer 2 and Layer 3 protocols further improve transaction speed and scalability by enabling off-chain processing while maintaining a secure blockchain environment [5]. Consequently, as e-commerce increasingly adopts these blockchain features, the architecture fortifies trust. It promotes transparency, as every transaction is recorded in an immutable ledger accessible to all participants, enhancing consumer confidence in digital transactions.

Performance evaluation

When evaluating the scalability and performance of cryptographic protocols in web-based transactions, distinct differences emerge between SSL/TLS and blockchain approaches. SSL/TLS, while predominantly favoured for its established and secure protocols, often struggles with issues related to centralized control and bottlenecks, particularly during peak transaction loads. As highlighted in, network authorities' secret keys are high-value targets for potential compromises, raising concerns about long-term scalability [11]. In contrast, blockchain technologies, primarily through implementations leveraging Layer 2 solutions, demonstrate remarkable potential to enhance scalability. The introduction of consensus mechanisms and zero-knowledge proofs allows for efficient transaction processing without sacrificing security, making blockchain an attractive alternative for large-scale e-commerce applications. For instance, decentralized storage enhances performance by distributing transactional loads, as illustrated in visualizations, which detail operational efficiencies across blockchain networks. Thus, integrating blockchain addresses scalability challenges and reinforces the security framework crucial for e-commerce resilience.

Key technologies for blockchain

Blockchain technology incorporates several critical components that enhance its efficacy in securing web-based transactions. Among these are consensus algorithms, which facilitate agreement among distributed network nodes, ensuring transaction legitimacy without needing a central authority. This decentralization mitigates risks inherent in SSL/TLS systems, such as single points of failure and reliance on centralized Certificate Authorities. Crucially, elliptic curve cryptography underpins blockchain security by providing robust encryption methods that facilitate secure key management and transaction privacy. Additionally, hash functions play a vital role in maintaining data integrity, as they create unique identifiers for each data block, enabling quick verification without exposing sensitive information. Moreover, zero-knowledge proofs allow parties to verify transaction authenticity without disclosing underlying data, thereby enhancing privacy a limitation frequently noted in conventional SSL/TLS transactions [6,10]. By integrating these technologies, blockchain presents a formidable alternative for secure e-commerce transactions, addressing many vulnerabilities associated with traditional models.

Scalability challenges

As digital transactions and e-commerce platforms gain momentum, the pressing need for effective scalability solutions becomes increasingly evident. A fundamental challenge with traditional SSL/TLS protocols is their centralized nature, often resulting in bottlenecks during peak transaction periods. This limitation impedes the system's capacity to efficiently handle many concurrent requests, risking potential slowdowns or failures [11]. By contrast, blockchain technology presents a more distributed architecture that inherently supports scalability through decentralized consensus mechanisms. Blockchain can allow thousands of transactions to be processed simultaneously, as seen in implementations leveraging Layer 2 solutions like rollups [2]. However, scalability remains a double-edged sword. At the same time, the technology promises vast improvements. Still, issues such as high transaction costs and latency in network confirmations are prevalent, especially in public blockchains, and they challenge their practical deployment in time-sensitive e-commerce scenarios. Consequently, addressing these scalability challenges is crucial for determining the viability of blockchain as a solution for secure web-based transactions (Figure 4).

Protocol	TransactionSpeed (transactions/second)	MaxConcurrentConnections	Latency (ms)	ScalabilityIssues
SSL/TLS	1000	5000	30	Limited by server capacity and SSL handshake overhead
Blockchain	15-30	Varies by network	300-1000	Network congestion, block size limitations

Figure 4: Scalability challenges for each protocol.

Results

Significant differences in security, scalability, and performance emerge in analyzing the effectiveness of SSL/TLS and blockchain-based approaches for securing web-based transactions. Findings illustrate that while SSL/TLS has long been the standard for web security, strengthening its framework with processes such as the handshake protocol and certificate authorities exposes it to centralized vulnerabilities and potential man-in-the-middle attacks. Conversely, blockchain technology demonstrates resilience by leveraging decentralized structures and immutable record- keeping, thus inherently reducing such central attack vectors. The comparison of these protocols indicates that blockchain can address scalability issues faced by SSL/TLS, especially in high- volume e-commerce environments, by employing layer two solutions to enhance transactional throughput. Moreover, by integrating advanced cryptographic techniques, including zero-knowledge proofs, blockchain presents robust mechanisms for achieving enhanced data privacy and integrity, highlighting its superior potential in modern transactional frameworks [5,10]. Overall, the results underscore blockchain's transformative possibilities over traditional SSL/TLS protocols in fostering secure and efficient e-commerce transactions.

Summary of findings

Significant insights emerge from the comparative analysis in evaluating the security frameworks and performance characteristics inherent in SSL/TLS and blockchain technologies. A key finding indicates that SSL/TLS has effectively facilitated secure transactions through its robust cryptographic mechanisms over the years.

However, due to its reliance on centralized certificate authorities, it remains vulnerable to specific attacks, such as Man-in-the-Middle (MITM) threats [3]. This centralization poses scalability bottlenecks, particularly in evolving e-commerce settings where transaction volumes surge. Conversely, blockchain technology has demonstrated a superior capacity for scalability and resilience. Utilizing decentralized structures mitigates risks associated with traditional security protocols by employing mechanisms like zero-knowledge proofs, which enhance privacy without compromising integrity [4]. The findings highlight blockchain's potential to address some security limitations associated with SSL/TLS, suggesting that its adoption could transform web-based transaction models and pave the way for more secure e-commerce frameworks.

Strengths and weaknesses

Several strengths and weaknesses emerge when evaluating the security frameworks of SSL/TLS and blockchain-based approaches, highlighting their respective capabilities in web transactions. SSL/TLS provides a robust, established method for securing data during transmission. Still, it suffers from vulnerabilities like reliance on trust-based Certificate Authorities and susceptibility to various attacks, including Man-in-the-Middle (MITM) incidents [7]. Conversely, blockchain presents a decentralized framework that enhances security through immutability and transparency, thus minimizing the risk of single points of failure. Its implementation of consensus mechanisms and cryptographic advancements, such as zero- knowledge proofs, fosters high integrity and operational trust [1]. However, scaling blockchain solutions can introduce latency, making them less efficient for high-volume transactions than SSL/TLS systems, which typically handle data exchanges swiftly despite their inherent risks. Ultimately, these frameworks showcase trade-offs between established performance and innovative security potential, necessitating further exploration into their integration within e- commerce systems [4].

Suggestions for future work and unresolved problems

While this analysis highlights the strengths of SSL/TLS and blockchain technologies in securing web-based transactions, several challenges and areas for improvement remain that warrant further exploration.

Hybrid Solutions: Future research could investigate the development of hybrid models combining SSL/TLS and blockchain technology to address the limitations of each system. For instance, a potential solution might involve using SSL/TLS for initial secure communication and employing blockchain for transaction validation and record-keeping. The optimization of consensus algorithms and integration of these two systems could lead to more efficient, scalable, and secure e-commerce platforms.

Blockchain Scalability Solutions: Blockchain technology's scalability is one of its major issues, particularly in e-commerce settings. Rollups and other Layer 2 solutions are still in the early stages of development despite their potential to increase transaction output. More effort is required to improve these systems, especially in settings with high transaction volumes, and to lower latency and related expenses. Some scalability problems with blockchain technology may also be resolved with research on Layer 3 protocols.

Performance Evaluation of Blockchain in Real-World E-Commerce: While the theoretical benefits of blockchain technology are apparent, additional observed research is required to assess how well it performs in practical e-commerce applications. Blockchain's usefulness and efficiency compared to conventional SSL/TLS systems could be better understood by testing it in various online shopping scenarios, including times when transactions are at their highest [12-28].

Unresolved problems

Blockchain has energy consumption issues despite its tremendous potential, particularly in Proof of Work systems and integrating with current e-commerce infrastructures. Additionally, there is still work to be done to resolve the difficulty of maintaining private keys and guaranteeing strong user authentication in decentralized systems. Before blockchain completely replaces or supplements SSL/TLS in commonplace e-commerce applications, this problem and continuing scalability and transaction speed challenges need to be fixed.

Conclusion

Integrating SSL/TLS and blockchain technologies presents unique solutions and challenges for securing web-based transactions. As evidenced through detailed comparisons, while SSL/TLS provides a robust framework utilizing public key cryptography to safeguard data transmission, it faces vulnerabilities, particularly in scalability and susceptibility to various cyber threats, such as Man-in-the-Middle (MITM) attacks. In contrast, blockchain technology establishes a decentralized and immutable system that enhances security by eliminating reliance on central authorities and mitigating many risks associated with traditional protocols. This research underscores blockchain's potential to address the significant security and scalability limitations of SSL/TLS, suggesting that a hybrid approach could optimize transaction security in e-commerce platforms. Ultimately, the findings indicate that blockchain's innovative mechanisms, including zero-knowledge proofs and decentralized validation, offer a promising way to develop secure online transactions, even as challenges remain in its practical implementation.

Conflicts of Interest

The authors declare no conflicts of interest in this research. The study was privately funded and independently conducted, with no influence from any external organizations or entities. All findings and conclusions reflect the authors' unbiased scientific efforts, ensuring the integrity and transparency of the research process.

References

1. Bulajoul W, James A, Li Y, Obande G, Shehu Y, et al. (2018) Security challenges and solutions for E- Business.
2. Aravind KA, Naik BR, Chennarao CS (2022) Combined digital signature with SHA hashing technique-based secure system: An application of blockchain using IoT. Turkish Journal of Computer and Mathematics Education (TURCOMAT) 13(3): 402-418. [Crossref]
3. Treiblmaier H, Sillaber C (2021) The impact of blockchain on e-commerce: A framework for salient research topics. Electronic Commerce Research and Applications 48: 101054. [Crossref] [GoogleScholar]
4. Sarfaraz A (2023) Blockchain-coordinated frameworks for scalable and secure supply chain networks. [Crossref] [GoogleScholar]
5. Bello G, Perez AJ (2019) Adapting Financial Technology Standards to Blockchain Platforms. ACMSE '19: Proceedings of the 2019 ACM Southeast Conference 109-116. [Crossref] [GoogleScholar]

6. Babel M, Sedlmeir J (2023) Bringing data minimization to digital wallets at scale with general- purpose zero-knowledge proofs. [Crossref] [GoogleScholar]
7. Molina F (2021) Constructing privacy aware blockchain solutions: Design guidelines and threat analysis techniques. [GoogleScholar]
8. Avik SC, Biswas S, Ahad MAR, Latif Z, Alghamdi A, et al. (2023) Challenges in blockchain as a solution for iot ecosystem threats and access control: A survey. [Crossref] [GoogleScholar]
9. Nguyen L, Tomy S, Pardede E (2024) Enhancing collaborative learning and e-mentoring in a smart education system in higher education. Computers 13(1): 28. [Crossref] [GoogleScholar]
10. Mammadzada K (2019) Blockchain Oracles.
11. Pereira FAS (2020) EPOS Security & GDPR Compliance.
12. Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, Choo KK (2020) An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Transactions on Services Computing 13(4): 625-638. [Crossref] [GoogleScholar]
13. Yazdinejad A, Srivastava G, Parizi RM, Dehghantanha A, Choo KK, et al. (2020) Decentralized authentication of distributed patients in hospital networks using blockchain. IEEE journal of biomedical and health informatics 24(8): 2146-2156. [Crossref] [GoogleScholar] [Pubmed]
14. Yazdinejad A, Dehghantanha A, Parizi RM, Srivastava G, Karimipour H (2023) Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks. Computers in Industry 144: 103801. [Crossref] [GoogleScholar]
15. Yazdinejad A, Dehghantanha A, Parizi RM, Hammoudeh M, Karimipour H, et al. (2022) Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks. IEEE Transactions on Industrial Informatics 18(11): 8356-8366. [Crossref] [GoogleScholar]
16. Dehghantanha A, Yazdinejad A, Parizi RM (2024) Autonomous cybersecurity: Evolving challenges, emerging opportunities, and future research trajectories. In Proceedings of the Workshop on Autonomous Cybersecurity 1-10. [Crossref] [GoogleScholar]
17. Mothukuri V, Parizi RM, Massa JL, Yazdinejad A (2024) An AI multi-model approach to DeFi project trust scoring and security. In 2024 IEEE International Conference on Blockchain (Blockchain) 19-28. [Crossref] [GoogleScholar]
18. Sorkhpour M, Yazdinejad A, Dehghantanha A (2024) Auto-CIDS: An autonomous intrusion detection system for vehicular networks. In Proceedings of the Workshop on Autonomous Cybersecurity 45-55. [Crossref]
19. Nazari H, Yazdinejad A, Dehghantanha A, Zarrinkalam F, Srivastava G (2024) P3GNN: A privacy-preserving provenance graph-based model for autonomous APT detection in software defined networking. In Proceedings of the Workshop on Autonomous Cybersecurity 34-44. [Crossref] [GoogleScholar]
20. Yazdinejad A, Bohlooli A, Jamshidi K (2018) Efficient design and hardware implementation of the OpenFlow v1.3 switch on the virtex-6 FPGA ML605. The Journal of Supercomputing 74: 1299-1320. [Crossref] [GoogleScholar]
21. Yazdinejad Abbas, Dehghantanha A, Parizi RM, Epiphaniou G (2023) An optimized fuzzy deep learning model for data classification based on NSGA-II. Neurocomputing 522: 116-128. [Crossref] [GoogleScholar]
22. Yazdinejad A, Dehghantanha A, Srivastava G (2023) AP2FL: Auditable privacy- preserving federated learning framework for electronics in healthcare. IEEE Transactions on Consumer Electronics. [Crossref] [GoogleScholar]
23. Yazdinejad A, Dehghantanha A, Srivastava G, Karimipour H, Parizi RM (2024) Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things." Journal of Systems Architecture 148: 103088. [Crossref] [GoogleScholar]
24. Namakshenas D, Yazdinejad A, Dehghantanha A, Srivastava G (2024) Federated quantum-based privacy-preserving threat detection model for consumer internet of things. IEEE Transactions on Consumer Electronics 70: 5829-5838. [Crossref] [GoogleScholar]
25. Nelles F, Yazdinejad A, Dehghantanha A, Parizi RM, Srivastava G (2024) A federated learning approach for multi-stage threat analysis in advanced persistent threat campaigns. arXiv. [Crossref] [GoogleScholar]
26. Namakshenas D, Yazdinejad A, Dehghantanha A, Parizi RM, Srivastava G (2024) IP2FL: Interpretation-based privacy-preserving federated learning for industrial cyber-physical systems. IEEE Transactions on Industrial Cyber-Physical Systems 2: 321-330. [Crossref] [GoogleScholar]
27. Yazdinejad A (2024) Secure and private ml-based cybersecurity framework for Industrial Internet of Things (IIOT). [GoogleScholar]
28. Yazdinejad A, Parizi RM, Dehghantanha A, Choo KKR (2020) P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. Computers & Security 88: 101629. [Crossref] [GoogleScholar]