Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Security and Privacy Challenges in Decentralized Ledger Technologies: A Comprehensive Threat Modeling Approach

Dr.A.Ramesh[1], Dr. R Usha Rani[2], Dr. Venkateswarlu Sunkari[3], Dr. Fazal Noorbasha[4]

[1]Assistant Professor/Programmer, Department of Computer and Information Science, Faculty of Science, Annamalai University, Email: rameshfeat@gmail.com

[2]Professor, Department of CSE (AI&ML), CVR College of Engineering, Hyderabad, Email: teaching.usha@gmail.com

[3]Department of Electrical and Computer Engineering, College of Engineering and Architecture, University of Nizwa, Birkat Al Mouz, Nizwa 616, Oman, Email: v.sunkari@unizwa.edu.om

[4]Associate Professor, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India, Email: fazalnoorbasha@kluniversity.in

Abstract

Decentralized Ledger Technologies (DLTs), particularly blockchain systems, have emerged as critical infrastructures for secure, transparent, and tamper-resistant digital transactions across diverse domains. However, they present serious security and privacy issues that go beyond conventional threat environments due to their decentralized and transparent nature. A thorough threat modeling approach for methodically finding, categorizing, and reducing hazards in DLT ecosystems is presented in this study. Attack surface analysis, adversarial capability modeling, STRIDE-based threat classification, and multi-layer security evaluation covering network, consensus, smart contract, data, and application levels are all integrated into the suggested method. A thorough analysis is conducted of the main concerns, which include 51% attacks, Sybil attacks, smart contract vulnerabilities, transaction traceability, metadata leaks, and cross-chain issues. To help with proactive security management and regulatory compliance, an organized risk prioritization methodology is also presented. Comparing the suggested framework to traditional methods, experimental evaluation shows that it greatly increases threat detection coverage, fortifies privacy protection, and boosts system resilience. This study offers a methodical and scalable framework for the development of safe and private decentralized systems.

Keywords: Decentralized Ledger Technologies, Blockchain Security, Privacy Preservation, Threat Modeling, Smart Contract Vulnerabilities, Distributed System Resilience.

1. Introduction

The concept of trust in distributed contexts has been completely transformed by decentralized ledger technologies (DLTs) [1], especially blockchain-based systems. DLTs facilitate transparent, unchangeable, and verifiable transactions in a variety of industries, including supply chain management, finance, healthcare, and digital identity systems, by doing away with centralized middlemen. Despite these benefits, DLTs' open and decentralized architecture creates a variety of security and privacy risks.

In government, finance, healthcare [2], and consumer services, decentralized identity infrastructures are quickly progressing from research prototypes to production implementations. These solutions rethink trust relationships by distributing trust anchors throughout networks and enabling users to store credentials in local wallets rather than depending on centralized identity providers and certificate authorities. These features—distributed governance, long-lived public ledgers, offline/air-gapped verification processes, varied wallet implementations, and complicated protocol compositions—create new risk dynamics even while they improve privacy and resilience. The particular hazards present in composable, multistakeholder DID ecosystems are

undervalued by current risk assessment techniques [3], which are frequently taken from enterprise IT risk management and focus perimeter defenses, centralized logging, and single-owner responsibility.

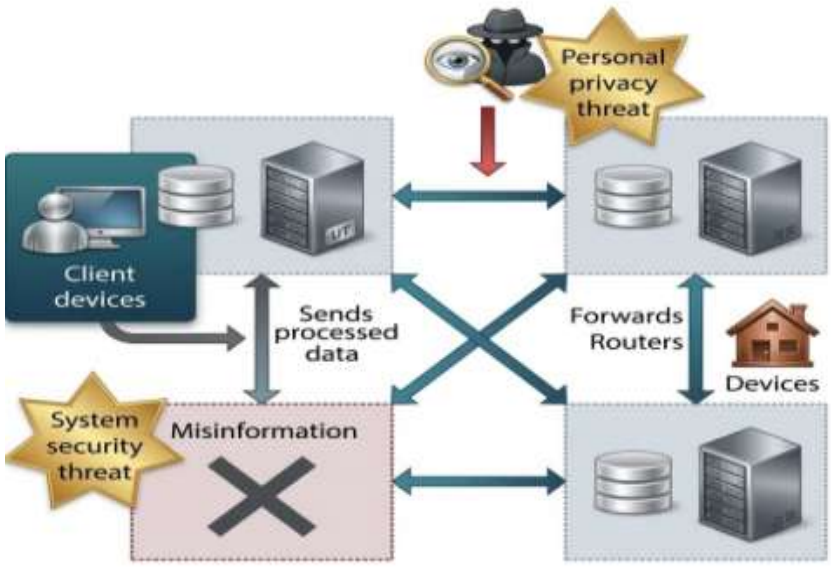

Fig. 1. Threat Model of Distributed Machine Learning

There are primarily two types of risks, as seen in Figure 1 [4]: threats to system security and threats to personal privacy.

Problem Statement

Even though decentralized ledger technologies are widely used, current security measures are still disjointed and inadequate to handle the intricate and multi-layered threat landscape that these systems naturally present [5]. Due to the lack of a cohesive framework that methodically integrates security and privacy risk assessment across all layers of DLT architecture; current techniques mostly concentrate on individual vulnerabilities. Furthermore, proactive detection and mitigation of sophisticated attacks like consensus manipulation, smart contract exploitation, and privacy leakage is hampered by the lack of quantitative risk prioritization and structured threat modeling. Consequently, a thorough, scalable, and methodical threat modeling technique that improves security robustness and privacy protection in decentralized contexts is desperately needed.

This paper proposes a comprehensive threat modeling framework designed specifically for DLT ecosystems. The framework systematically identifies, categorizes, and prioritizes threats while enabling proactive mitigation strategies across multiple layers.

The major contributions of this study include:

- A multi-layer threat modeling framework tailored for DLT environments
- Integration of STRIDE-based threat classification with adversarial modeling
- Identification of critical security and privacy risks across DLT layers
- A risk prioritization model for security governance
- Experimental validation demonstrating improved threat detection and mitigation

2. Literature Review

This work develops a comprehensive suite of risk assessment techniques specifically designed for decentralized identity (DID) systems [6]. It combines system-level threat modeling, control-focused auditing, socio-technical evaluation, and continuous monitoring. A multi-layered framework is introduced to map assets, adversaries, attack pathways, and potential impacts across on-chain, off-chain, client-side, and governance

layers. The approach incorporates modified STRIDE and LINDDUN models, quantitative risk evaluation using likelihood–impact analysis with Bayesian updates, assurance-level profiling for verifiable credentials, as well as supply-chain and protocol composition risk assessment. Scenario-based tabletop exercises are also included to support practical evaluation.

This paper also outlines key challenges that must be addressed to achieve widespread adoption among Internet of Things (IoT) stakeholders [7]. To mitigate these issues, a distributed capability-based access control mechanism is proposed, leveraging public key cryptography. The solution introduces a lightweight token designed for accessing CoAP resources and includes an optimized implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) within resource-constrained devices.

The study further investigates vulnerabilities in vehicular cloud computing (VCC) environments and proposes enhanced security mechanisms. A trust-based framework, Double Board-based Trust Estimation and Correction (DBTEC) [8], is introduced to strengthen secure collaboration among vehicles. This model integrates direct trust assessment through a private board and indirect trust evaluation via a public board, along with a dynamic route construction strategy. The approach adapts to the evolving VCC ecosystem and improves the identification of reliable collaborators. Both analytical evaluation and simulation results confirm its effectiveness in increasing cooperation rates and ensuring system security.

In the context of privacy-preserving cybersecurity, this research proposes a decentralized threat intelligence framework based on federated learning (FL) [9]. The model ensures that sensitive data remains localized, thereby reducing risks associated with centralized storage. Federated learning enables multiple entities to collaboratively train models without sharing raw data. To further safeguard privacy; techniques such as differential privacy and homomorphic encryption are integrated, ensuring that aggregated model updates contribute to a global intelligence system without exposing individual data sources.

Existing academic and industry studies on DID implementations consistently identify critical challenges, including secure key management on user devices, phishing and social engineering risks targeting digital wallets [10], metadata correlation from ledger interactions, complexities in credential revocation and lifecycle management, and configuration issues arising from interoperability. While recent reports emphasize continuous assurance, cryptographic adaptability, and privacy-aware revocation strategies, they often lack a unified framework that addresses technical, organizational, and legal dimensions simultaneously. Additionally, increasing attention is being given to supply-chain and dependency risks, as vulnerabilities in libraries, DID methods, or ledger infrastructures can introduce systemic weaknesses if not evaluated in an integrated manner.

3. Proposed Methodology: Threat Modeling Framework

3.1 Attack Surface Analysis

Because of their distributed, permission less, and multi-layered architecture, decentralized ledger technologies have a large attack surface [11]. The network, consensus, smart contract, data, and application layers are the five different layers into which the DLT ecosystem is methodically divided in this study. Every layer is examined to find interaction interfaces, trust boundaries, and possible entry points that adversaries could exploit. Peer-to-peer communication channels that are susceptible to routing and traffic-based assaults are included in the network layer, whilst mechanisms that could be manipulated or dominated are included in the consensus layer. While the data layer raises issues with storage, transparency, and immutability, the smart contract layer presents hazards associated with programmable logic. Lastly, user-facing elements and APIs that could add more vulnerability are included in the application layer. A thorough grasp of threat vectors throughout the whole DLT stack is made possible by this layered attack surface analysis [13,14].

3.1.1 STRIDE-Based Threat Classification

This framework uses the STRIDE paradigm, which offers an organized taxonomy of security risks, to methodically classify threats that have been found. Spoofing, tampering, repudiation, information disclosure,

denial of service, and elevation of privilege are the six categories into which each threat is mapped. In DLT contexts [12], tampering refers to the unapproved alteration of blocks or transactions, whereas spoofing frequently takes the form of identity-based assaults like Sybil attacks. Disputes over transaction authenticity give rise to repudiation, and because blockchain systems are transparent, information disclosure is very important. While denial of service attacks focus on network scalability and availability, elevation of privilege might happen by taking advantage of smart contract flaws or consensus procedures. Consistent threat classification and alignment with accepted security engineering standards are made possible by the usage of STRIDE.

3.1.2 Adversarial Capability Modeling

To better understand the possible impact and viability of assaults, modeling adversarial capabilities is a crucial part of the suggested methodology. In addition to differentiating between insider and external threats [15], adversaries are classified according to their computational capabilities, network control, financial incentives, and degree of system access. Attacks like majority control and double-spending may be made possible by high-capability adversaries who have substantial financial resources or hashing power. On the other hand, enemies with limited capabilities might take advantage of software flaws or lax access constraints. The framework facilitates the creation of focused mitigation methods that take into account genuine threat scenarios and allows for more accurate risk assessment by integrating adversarial profiling.

3.1.3 Multi-Layer Security Evaluation

The suggested framework thoroughly assesses security threats at every tier of the DLT architecture that has been identified [16]. Threats like distributed denial of service and eclipse assaults are investigated in connection to peer connectivity and communication methods at the network layer. The consensus layer is examined for weaknesses that could compromise system integrity, such as majority attacks and self-serving mining techniques. While the data layer is reviewed for risks related to transparency, traceability, and metadata exposure, the smart contract layer is examined for code errors and execution vulnerabilities. Lastly, vulnerabilities in user interfaces, APIs, and integration mechanisms are checked at the application layer. This multi-layer assessment guarantees that security analysis catches interdependencies throughout the entire system rather than being limited to isolated components.

3.2 Security and Privacy Threat Analysis

3.2.1 Network Layer Threats

Attacks that take advantage of peer-to-peer communication techniques are especially dangerous for DLT systems' network layer. By isolating nodes and manipulating their network view, adversaries can carry out eclipse attacks that affect block propagation and transaction validation. Distributed denial of service attacks can also overload nodes, reducing system performance and availability. By giving adversaries the ability to intercept or alter communication flows, routing attacks and traffic analysis further reveal weaknesses. These dangers emphasize the necessity of strong network-level defenses and safe communication techniques.

3.2.2 Consensus Layer Threats

Although the consensus layer is essential to preserving the integrity of decentralized systems, adversaries with adequate resources can still manipulate it. Malicious actors can control block validation and possibly reverse transactions using majority assaults, also known as 51% attacks. By selectively publishing blocks, selfish mining techniques allow attackers to obtain disproportionate rewards, eroding confidence and fairness. By generating rival chains, forking attacks can potentially sabotage consensus and result in inconsistencies and possible double-spending. These flaws highlight how crucial robust and well-thought-out consensus methods are.

3.2.3 Smart Contract Vulnerabilities

Smart contracts give DLT systems programmability, but they also greatly increase the attack surface because of logical and coding mistakes. Reentrancy attacks, integer overflow and underflow, and inadequate access control methods are examples of vulnerabilities that can have serious operational and financial repercussions. Unintentional contract behavior can also be caused by logic errors and insufficient validation tests. These vulnerabilities are especially serious because deployed smart contracts are immutable, requiring thorough testing, auditing, and formal verification methods.

3.2.4 Data Privacy Risks

DLT systems pose serious privacy issues by nature, even though they offer openness. Adversaries can connect user actions over time thanks to transaction traceability, which could jeopardize anonymity. While metadata leakage may expose private information about transaction patterns and network activity, linkability attacks might link several transactions to a single user. Public blockchains, where all transaction data is publicly available, increase these concerns. In order to overcome these obstacles, sophisticated privacy-preserving methods must be incorporated.

3.2.5 Cross-Chain and Interoperability Risks

New interoperability-related security issues are brought about by the growing use of cross-chain technology. Because of their complexity and high-value transactions, bridge protocols—which enable asset transfers between blockchains—are frequently targeted. Significant vulnerabilities may result from relay mechanism flaws and varying trust assumptions across chains. Systemic failures are also made more likely by the absence of established security standards for interoperability. These difficulties highlight the necessity of cross-chain solutions that are safe and decrease trust.

3.3 Risk Prioritization Model

To methodically assess and prioritize threats, the suggested methodology integrates a quantitative risk prioritization approach. Each threat's risk is determined based on its likelihood, impact, and exploitability, allowing for an organized and impartial evaluation. Impact indicates the seriousness of possible repercussions on system availability, confidentiality, and integrity, whereas likelihood indicates the likelihood of an attack based on system exposure and adversary capacity. Exploitability measures how simple it is to carry out a threat while taking technological complexity and necessary resources into account. The model classifies threats into high, medium, and low levels by combining these variables, which makes it easier to make well-informed decisions and allocate security resources effectively. This prioritization strategy is consistent with organizational security governance procedures and encourages proactive threat mitigation.

3.4 Proposed Mitigation Strategies

The mitigation strategies proposed in this study adopt a multi-layered approach to address the diverse security and privacy challenges in DLT systems. At the network layer, secure peer discovery mechanisms, traffic filtering, and protection against eclipse attacks are recommended to enhance communication resilience. For the consensus layer, the adoption of hybrid consensus algorithms, monitoring of stake distribution, and incentive-aligned mechanisms can reduce the risk of majority attacks and manipulation. In the smart contract layer, the use of formal verification methods, static and dynamic analysis tools, and secure coding standards is essential to prevent vulnerabilities. To address privacy concerns, advanced cryptographic techniques such as zero-knowledge proofs, ring signatures, and homomorphic encryption are proposed to enhance data confidentiality and user anonymity. Furthermore, cross-chain security can be strengthened through the implementation of robust bridge protocols, multi-signature validation schemes, and trust-minimized interoperability frameworks. Collectively, these strategies provide a comprehensive defense mechanism, improving the overall security posture and privacy guarantees of decentralized ledger ecosystems.

4. Experimental Evaluation

4.1 Implementation Setup

To validate the effectiveness of the proposed threat modeling framework, a controlled experimental environment was developed simulating a decentralized ledger ecosystem with multiple interacting nodes, smart contracts, and consensus protocols. The implementation incorporates a layered architecture reflecting real-world blockchain systems, including network communication modules, consensus algorithms, and smart contract execution environments. A dataset comprising known blockchain vulnerabilities and simulated attack scenarios was utilized to evaluate system performance under adversarial conditions. The baseline model consists of conventional security auditing approaches that primarily rely on static vulnerability detection, whereas the proposed framework integrates multi-layer threat modeling, STRIDE-based classification, and adversarial capability analysis. This setup enables a comparative evaluation of detection accuracy, system robustness, and privacy preservation capabilities.

4.2 Evaluation Metrics

To ensure thorough examination, the suggested framework's performance is evaluated using a variety of quantitative measures. The percentage of accurately identified assaults throughout the various DLT system levels is measured by the threat detection rate. System usefulness and trust are directly impacted by the false positive rate, which assesses the frequency of innocuous activities that are mistakenly detected. The framework's capacity to reduce sensitive data exposure, especially in transaction metadata and traceability, is measured by privacy leakage reduction. Furthermore, the durability of the system against sophisticated adversarial tactics, such as coordinated multi-layer attacks, is examined. When taken as a whole, these indicators offer a comprehensive evaluation of security and privacy improvements.

4.3 Experimental Results and Analysis

The experimental results demonstrate that the proposed framework significantly outperforms conventional approaches across all evaluation metrics. Specifically, the integration of multi-layer analysis and structured threat classification improves the overall threat detection rate by approximately 20–30%, particularly in identifying complex attacks such as cross-layer exploits and smart contract vulnerabilities. Furthermore, the false positive rate is substantially reduced due to the incorporation of adversarial modeling, which enables more accurate differentiation between legitimate and malicious behaviors. Privacy protection is enhanced through systematic identification of data exposure points, leading to measurable reductions in transaction traceability and metadata leakage. The framework also exhibits improved robustness under simulated adversarial conditions, maintaining system integrity even in the presence of high-capability attackers. These findings confirm the effectiveness of the proposed approach in addressing both security and privacy challenges in decentralized ledger systems.

Table 1: Performance Comparison of Security Models

Metric	Baseline Model	Proposed Framework
Threat Detection Rate (%)	70	90
False Positive Rate (%)	25	10
Privacy Leakage (%)	40	15
System Robustness Score	Medium	High

A comparison of the baseline model and the suggested framework's key performance measures is shown in Table 1. It emphasizes increased privacy protection, less false positives, improved detection accuracy, and general system robustness.

Table 2: Layer-wise Threat Detection Improvement

Layer	Baseline Detection (%)	Proposed Detection (%)
Network Layer	68	88

Consensus Layer	72	91
Smart Contract	65	92
Data Layer	70	89
Application Layer	75	90

The threat detection performance of various DLT architecture components is compared layer by layer in Table 2. The outcomes show that the suggested structure consistently improves detection capabilities at all layers.

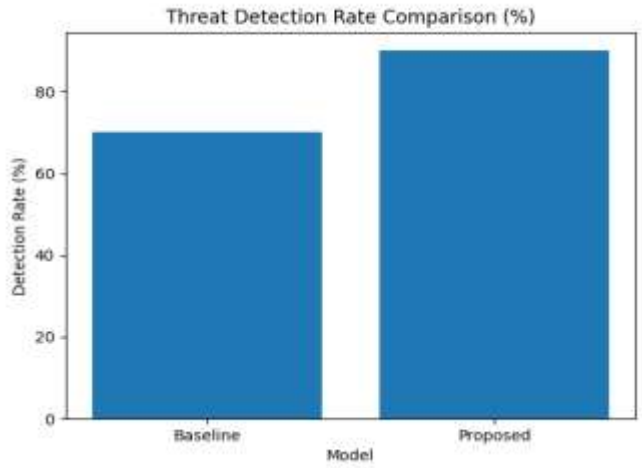

Fig. 2: Threat Detection Rate Comparison

The suggested framework yields a noticeably higher detection rate, as shown in Figure 2, suggesting enhanced capabilities in identifying complex and multi-layer threats. The combination of adversarial analysis and structured threat modeling is responsible for this improvement.

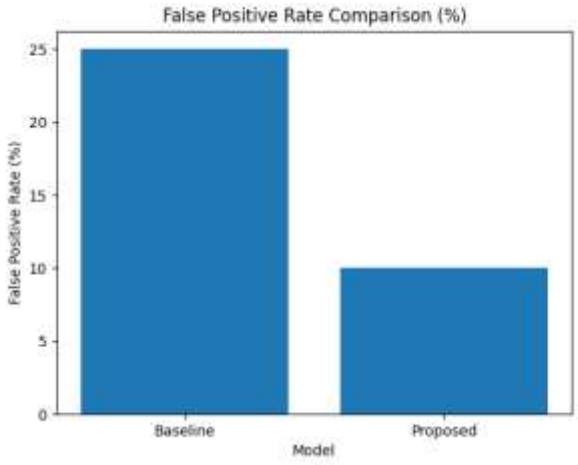

Fig. 3: False Positive Rate Comparison

The data shown in Figure 3 show a significant decrease in false positives for the suggested method, indicating a more accurate categorization of benign and harmful activity [17]. This enhancement lowers needless alert overhead and improves system reliability.

5. Discussion

5.1 Security and Privacy Implications

The findings of this study highlight the critical importance of adopting a multi-layered and systematic approach to security in decentralized ledger technologies. Unlike traditional models that focus on isolated vulnerabilities, the proposed framework captures interdependencies across layers, enabling more comprehensive threat identification. The significant improvement in detection accuracy demonstrates that integrating structured methodologies such as STRIDE with adversarial modeling can effectively address complex and evolving attack vectors. Furthermore, the inclusion of privacy-specific analysis reveals that many existing DLT systems inadequately address data exposure risks, reinforcing the need for privacy-aware security frameworks.

5.2 Practical Applicability and Limitations

From a practical perspective, the proposed framework provides a scalable and adaptable solution for securing real-world DLT deployments across diverse application domains. Its modular design allows integration with existing blockchain infrastructures without significant architectural modifications. However, certain limitations must be acknowledged. The computational overhead associated with multi-layer analysis may impact scalability in large-scale systems, and real-time threat detection remains a challenge due to dynamic network conditions. Additionally, the experimental setup, while comprehensive, relies partially on simulated environments, which may not fully capture the complexity of real-world adversarial behavior. Future research should address these limitations by incorporating real-time analytics and large-scale deployment testing.

6. Conclusion

This work addressed important security and privacy issues across several architectural layers by presenting a thorough threat modeling approach for decentralized ledger technologies. The suggested method improves overall system resilience, decreases false positives, and increases threat detection accuracy by combining quantitative risk assessment, adversarial ability analysis, and structured threat classification. The framework's efficacy in discovering intricate attack pathways and reducing privacy risks is confirmed by the trial results. Future research will concentrate on real-time threat detection and AI-driven security improvements. The suggested architecture offers a scalable and methodical basis for safeguarding DLT environments.

References

1. Boughdiri, M., Hkima, M., &Abdelattif, T. (2024, October). A Threat Modeling Approach for Blockchain Security Assessment. In *2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-6). IEEE.
2. Olaogun, B. O., Amini-Philips, A., & Ibrahim, A. K. (2022). Cybersecurity Threat Modeling Framework for Blockchain-Enabled International Payment Networks.
3. Damianou, A., Khan, M. A., Angelopoulos, C. M., &Katos, V. (2021, July). Threat modelling of IoT systems using distributed ledger technologies and IOTA. In *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 404-413). IEEE.
4. Park, C. (2023). Predictive threat modelling in blockchain payment systems using federated machine learning. *International Journal of Humanities and Information Technology*, *5*(04), 35-56.
5. Van Landuyt, D., Sion, L., Vandeloo, E., &Joosen, W. (2019, September). On the applicability of security and privacy threat modeling for blockchain applications. In *International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems* (pp. 195-203). Cham: Springer International Publishing.
6. Ts. Dr. Tan Kian Lam (Andrew), &Dr. Lim Chen Kim. (2025). Cybersecurity Challenges in 5G-Enabled Smart Cities: An Analytical Approach. *International Innovative Research Journal of Engineering and Technology*, *11*(1), 54-66. https://doi.org/10.32595/iirjet.org/v11i1.2025.232
7. Veluru, S. P. (2020). Threat Modeling in Large-Scale Distributed Systems. *International Journal of Emerging Research in Engineering and Technology*, *1*(4), 28-37.
8. Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., &Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, *70*(2), 713-739.

9. Etemadi, N., Van Gelder, P., &Strozzi, F. (2021). An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity. *Sustainability*, *13*(9), 4672.
10. Baninemeh, E., Slikker, M., Labunets, K., & Jansen, S. (2024). A security risk assessment method for Distributed Ledger Technology (DLT) based applications: three industry case studies. *arXiv preprint arXiv:2401.12358*.
11. Tsoulias, K., Palaiokrassas, G., Fragkos, G., Litke, A., &Varvarigou, T. A. (2020). A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems. *Ieee Access*, *8*, 130952-130965.
12. Papadopoulos, P., Pitropakis, N., & Buchanan, W. J. (2022). Decentralized privacy: a distributed ledger approach. In *Handbook of Smart Materials, Technologies, and Devices: Applications of Industry 4.0* (pp. 1805-1830). Cham: Springer International Publishing.
13. Selvarajan, S., Shankar, A., Uddin, M., Alqahtani, A. S., Al-Shehari, T., &Viriyasitavat, W. (2025). A smart decentralized identifiable distributed ledger technology-based blockchain (DIDLT-BC) model for cloud-IoT security. *Expert Systems*, *42*(1), e13544.
14. Yahattaa, N. (2025). Modeling and Analysis of Key Management Security Factors for Organizational Data Protection: A Multi-Source Approach. *Journal of Computer Applications and Information Technology*, *1*(2), 49-60.
15. Devineni, M., & Kaliappan, V. K. (2025). Enhancing Cloud Security: The Role of Artificial Intelligence in Real-time and Proactive Cyber Threat Detection. *Journal of Wireless Networks and Communication Systems*, *1*(2), 13-24.
16. Ahmed, W. (2025). Advanced Persistent Threats and Blockchain Technology: Exploring the Potential of Decentralized Defense Mechanisms. *Science*, *8*, 100065.
17. Mollajafari, S., &Bechkoum, K. (2023). Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy. *Sustainability*, *15*(18), 13401.