iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70340

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

A Conceptual Framework for Cybersecurity Threat Intelligence Sharing Using Blockchain-Based Systems

Saket Pradhan[1], Debharghya Biswas[2]
Faculty of Computer Science & IT, Kalinga University, Raipur, India

Abstract: ***Cybersecurity threat intelligence (CTI) is essential for identifying and mitigating cyberattacks. However, traditional CTI sharing mechanisms struggle with issues such as trust, data integrity, and stakeholder collaboration. This paper examines how blockchain technology can revolutionize CTI sharing through its inherent features of decentralization, immutability, and transparency. We propose a conceptual blockchain-based framework that facilitates secure and efficient threat intelligence exchange. The paper discusses theoretical foundations, outlines benefits and limitations, and suggests directions for practical implementation. Our findings indicate that blockchain technology holds significant promise for building a more resilient and trusted cybersecurity ecosystem.***
Keywords: Blockchain, BlocTIShare, Cybersecurity, Decentralized, Threat Intelligence

I. INTRODUCTION

Contemporary digital operations witness significantly growing frequencies and sophistication levels of cyberattacks that continuously endanger essential critical services, financial systems, and national defense facilities. Cybersecurity threat intelligence (CTI) has arisen as a forward-thinking defensive tool to deliver meaningful threat information about attackers, along with signs of system breaches and modernized attack methods. CTI information exchange between organizations serves as a strategic requirement to build up collective cyber resilience based on current research by ENISA 2021 and Shackleford 2020.

Organizations experience challenges when they attempt to implement inter-organizational threat intelligence sharing programs in practice. Organizations face key difficulties during CTI sharing, including trust challenges alongside data integrity concerns, as well as interoperability problems alongside regulatory compliance requirements. Multiple organizations refrain from sharing intelligence because they want to protect themselves from potential data misuse and reputational harm as well as legal exposure, according to (Pawlicka et al. 2019). CTI sharing systems operated as centralized entities create system weaknesses and face threats from insider actions as well as government monitoring and censorship, according to (Cichonski et al. 2021).

Recent research suggests that blockchain, a decentralized, immutable, and transparent ledger technology, could offer a promising solution to these limitations (Conti et al., 2018; Christidis & Devetsikiotis, 2016). By distributing data storage and decision-making, blockchain can eliminate the need for centralized trust brokers and enable tamper-evident record-keeping. Furthermore, smart contracts embedded within blockchain networks can automate and enforce access control policies, incentivize information sharing, and mitigate risks associated with human error or malicious intent.

This paper proposes a conceptual framework for a blockchain-based cybersecurity threat intelligence sharing system. The goal is to address the enduring issues of trust, data integrity, and access control that hinder current CTI sharing efforts. The proposed model leverages the core principles of blockchain technology, decentralization, transparency, and immutability to create a more secure, verifiable, and collaborative threat-sharing environment. While not intended as a technical implementation guide, the framework aims to provide a foundation for future empirical research, prototype development, and cross-sectoral policy discussions.

A. Problem Statement

In an era of increasingly sophisticated and cross-border cyber threats, effective cybersecurity threat intelligence (CTI) sharing is critical to enabling timely detection and collective defense. However, current CTI sharing practices face significant limitations, including a lack of trust among stakeholders, data privacy concerns, the absence of clear incentives, and reliance on centralized architectures that are vulnerable to single points of failure. These challenges often lead to fragmented, delayed, or withheld intelligence, thereby weakening collaborative cybersecurity efforts.

Although blockchain technology offers promising features such as decentralization, immutability, and programmable trust through smart contracts, there remains a conceptual gap in applying it systematically to address the specific barriers in CTI sharing. Therefore, this study seeks to develop a conceptual framework for blockchain-enabled CTI sharing that enhances trust, preserves data confidentiality, incentivizes participation, and fosters secure, real-time collaboration across organizations and sectors.

B. Research Objectives

In this study, we aimed to contribute to the growing conversation on blockchain in cybersecurity by:

1) Proposing a novel conceptual framework for CTI sharing using blockchain, focusing on interoperability, trust, and governance.
2) Synthesizing existing technical and organizational models into a unified architecture that incorporates smart contracts, consent-based data sharing, and reputation mechanisms.
3) Offering a foundation for future empirical validation, policy discussions, and technical prototyping.

II. LITERATURE REVIEW

A. Existing Approaches to Cybersecurity Threat Intelligence (CTI) Sharing

The concept of threat intelligence sharing is grounded in the belief that collaborative defense yields better security outcomes than siloed protection. Standards like STIX (Structured Threat Information Expression) and TAXII (Trusted Automated eXchange of Indicator Information) were introduced to facilitate this (MITRE, 2021). These standards allow structured, machine-readable data exchange about indicators of compromise (IOCs), attack vectors, and threat actor behaviour across different platforms.

Studies such as Husák et al. (2018) and Tounsi & Rais (2018) highlight the benefits of CTI, including improved detection speed and contextualization of threats. However, these studies also stress persistent barriers: lack of trust between organizations, fear of reputational damage, and regulatory hurdles (e.g., data protection laws). ENISA's Threat Landscape Report (2021) confirms that although technical mechanisms exist, adoption is limited, and most threat-sharing remains voluntary and informal.

Additionally, centralized platforms like Information Sharing and Analysis Centres (ISACs) and government-run portals (e.g., DHS's AIS program) suffer from issues of latency, trust, and single points of failure (Pawlicka et al., 2019).

Key Limitation Identified: Most current CTI-sharing models rely on centralized intermediaries, which inherently contradict the principle of distributed trust and expose systems to compromise.

B. Blockchain in Cybersecurity: A Growing Landscape

Blockchain has emerged as a trustless trust mechanism, where consensus is achieved algorithmically rather than through third-party validation. The literature is increasingly exploring blockchain in cybersecurity, with focus areas including:

1) Secure audit trails (Yli-Huumo et al., 2016),
2) Digital identity and authentication (Christidis & Devetsikiotis, 2016),
3) IoT security (Conti et al., 2018),
4) Data provenance and access control (Ali et al., 2021).

In terms of threat intelligence, some scholars have begun conceptualizing blockchain-based solutions. For instance, Cheng et al. (2020) proposed *CyberChain*, a prototype CTI system leveraging Hyperledger Fabric, aimed at improving data integrity and accountability. However, they noted the lack of incentives for participation and scalability constraints.

Similarly, Ma et al. (2021) explored the use of blockchain for malware intelligence sharing, but the framework lacked robust governance mechanisms or privacy-preserving features, limiting its practicality in real-world deployment.

Es-Samaali et al. (2023) offered a meta-analysis of blockchain applications in cybersecurity and concluded that most proposed models remain in a theoretical or experimental stage, with few achieving sustained deployment due to interoperability, latency, or privacy concerns.

C. The Trust Problem in CTI Sharing

A central theme across literature is the trust paradox, while threat intelligence sharing requires collaboration, organizations are reluctant to share due to mistrust. Tounsi & Rais (2018) classify trust issues as either organizational (e.g., competition, fear of leaks) or technical (e.g., data misuse, insider threats).

Blockchain's cryptographic guarantees and distributed consensus can mitigate some technical trust issues, but organizational trust remains a soft constraint. Addressing this may require introducing reputation systems, smart contract-based access policies, and selective disclosure mechanisms, all of which are still under-explored in current research.

III. METHODOLOGY

This study adopts a conceptual and exploratory research methodology, which is appropriate for the investigation of emerging technologies, frameworks, and theoretical models that are still evolving. The objective is to construct a novel conceptual framework for secure, trustworthy, and efficient cybersecurity threat intelligence (CTI) sharing using blockchain technology, grounded in existing literature, standards, and observed challenges in real-world cyber threat intelligence ecosystems.

The research design is qualitative, relying primarily on secondary data from academic literature, technical reports, and industry whitepapers. Sources include peer-reviewed publications from IEEE, ACM, Springer, and Elsevier, alongside security standards such as STIX and TAXII, and documentation on blockchain platforms like Ethereum and Hyperledger Fabric. Through a critical review of these materials, existing limitations in CTI sharing, such as data sensitivity, lack of trust, and insufficient incentives, are identified and used to inform the proposed framework.

The development of the conceptual framework followed four iterative phases. First, a systematic literature review was conducted to identify gaps in current CTI sharing mechanisms, particularly around trust, privacy, and interoperability. Second, a requirement analysis was performed to determine the technical and organizational needs of a secure and scalable intelligence sharing system. These included attributes like decentralized access control, privacy-preserving protocols, immutable logging, and incentive structures. Third, a high-level architectural model was designed, comprising a consortium blockchain network, smart contracts, reputation systems, and off-chain storage for scalable and secure data handling. The architecture was visualized in a conceptual diagram to illustrate the interactions among components and stakeholders.

Finally, the proposed model was evaluated theoretically by mapping its components to established principles such as Privacy by Design (PbD), Zero Trust Architecture (ZTA), and the blockchain trilemma (balancing decentralization, scalability, and security). While this paper does not include empirical validation, the framework offers a robust foundation for future pilot implementations and experimental studies. Ethical considerations, including data sensitivity and regulatory compliance (e.g., with GDPR), were also integrated into the framework design to ensure responsible and lawful threat intelligence exchange.

IV. CONCEPTUAL FRAMEWORK

A. Overview of the Proposed Framework

The proposed conceptual framework, termed **"BlocTIShare"** (Blockchain Threat Intelligence Sharing), is a blockchain-based system designed to facilitate secure, privacy-preserving, and incentive-driven sharing of cybersecurity threat intelligence (CTI) among trusted participants in a decentralized environment.

Objective:

To build a decentralized, tamper-resistant infrastructure that enables:

1) Verified sharing of threat intelligence (indicators of compromise, attack vectors, malware signatures),
2) Fine-grained access control and data governance via smart contracts,
3) Contributor reputation tracking and incentives,
4) Compatibility with existing CTI data standards (e.g., STIX).

B. Architecture Components

The BlocTIShare framework consists of the following seven primary components, as summarized in Table 1.

Component	Function
1. Permissioned Blockchain Network	A consortium ledger (e.g., using Hyperledger Fabric) that ensures only vetted institutions (banks, CERTs, ISACs, telecoms) can participate.
2. CTI Nodes	Each organization operates a node that can submit, validate, and query threat intelligence.

3. Smart Contract Layer	Governs sharing policies, access control rules, and incentive distribution through automated enforcement.
4. STIX Parser & Formatter	Converts structured threat data into interoperable STIX 2.1 format before committing to the blockchain.
5. Off-Chain Storage (e.g., IPFS)	Used to store large CTI payloads (e.g., malware samples, full logs), with only content hashes stored on-chain for integrity.
6. Access Control & Encryption Engine	Implements attribute-based encryption (ABE) and zero-knowledge proofs (ZKP) to allow selective data access.
7. Reputation & Incentive Module	Tracks the accuracy, frequency, and usefulness of contributions; awards tokens or reputational scores to high-quality contributors.

Table 1: Proposed system key components.

C. System Workflow

Here's how a threat intelligence submission and sharing process would work in BlocTIShare:

1) Threat Detection

An organization detects a potential threat (e.g., phishing domain, malware hash, DDoS source IP).

2) Data Formatting & Privacy Enforcement

The CTI is parsed into STIX format. Sensitive fields are encrypted. Contributor sets access parameters (e.g., "share with all telecoms except competitors").

3) Smart Contract Invocation

A smart contract is triggered that:

- Validates submission format,
- Checks contributor credentials and history,
- Logs the CTI hash and metadata to the blockchain,
- Updates contributor's reputation metrics.

4) Off-Chain Storage and Reference Hashing

The full data payload is uploaded to a decentralized file system (e.g., IPFS); only the content hash and metadata are stored on-chain for integrity checks.

5) Access Request and Policy Enforcement

A peer node requests access to CTI data. The smart contract evaluates requestor eligibility (based on the contributor's policy) and grants access if conditions are met.

6) Reputation Feedback

After using the intelligence, recipient organizations rate its usefulness. Reputation scores update to reflect trustworthiness and contribution quality.

Figure 1 describes how this will work within an organization setting.

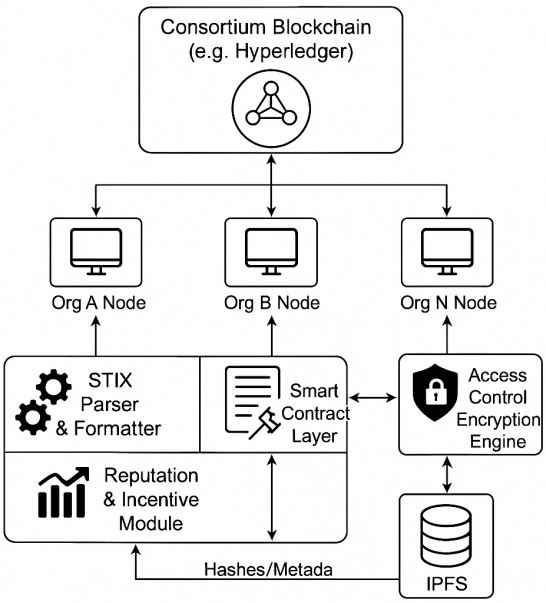


Figure 1: The System Workflow

D. Comparison with the existing system.

To confirm the effectiveness of our proposed system, we perform a comparison check with the popular existing system, CyberChain, and the analysis indicates a significant improvement in our system. Table 2 presents a summary of the comparison analysis.

Feature	Centralized ISACs	CyberChain (2020)	BlocTIShare (Proposed)
Trust Model	Manual agreements	Blockchain-based	Blockchain + Smart Contracts
Access Control Granularity	Basic (Role-based)	Organization-level	Attribute-Based, Contributor-defined
Data Format	Varies	JSON	STIX 2.1-Compliant
Contributor Incentives	None	None	Token-based + Reputation
Privacy Mechanisms	NDA, legal contracts	Basic hashing	Encryption + ZKP
Interoperability	Low	Medium	High (STIX/TAXII Compatible)

Table 2: Comparison Analysis.

V. DISCUSSION

The conceptual framework proposed in this study represents a paradigm shift in how cybersecurity threat intelligence (CTI) can be shared across organizations, sectors, and jurisdictions. By leveraging blockchain technology, the model addresses long-standing challenges associated with centralized CTI systems, such as a lack of trust, data manipulation risks, and limited transparency. The integration of a permissioned blockchain enables a decentralized yet controlled environment where participants can contribute, access, and verify threat data without relying on a single point of authority.

One of the key contributions of this framework is its emphasis on trustless collaboration. Traditional CTI sharing models depend heavily on bilateral trust agreements or central authorities, which are both costly and difficult to scale. Blockchain's decentralized consensus mechanism replaces this need with cryptographic verification, ensuring that threat data integrity is maintained while fostering cooperation among potentially competing entities. Moreover, the use of smart contracts allows for the automatic enforcement of sharing policies, access controls, and incentive mechanisms, thus reducing reliance on manual administrative overhead and enhancing compliance with organizational policies.

In terms of privacy and confidentiality, the framework strikes a balance between information transparency and data protection. Through the use of off-chain storage and zero-knowledge proofs or other privacy-preserving techniques (e.g., selective disclosure or homomorphic encryption), sensitive threat data can be selectively shared without compromising the privacy of the originating entity. This is especially critical for sectors such as finance, healthcare, and government, where the exposure of certain threat indicators or metadata could violate compliance obligations or reveal internal vulnerabilities.

The framework also introduces the concept of incentivized participation, a novel but essential feature in the CTI sharing ecosystem. Historically, organizations have been reluctant to share intelligence unless there is a clear benefit. By incorporating a reputation or token-based incentive model governed by smart contracts, the framework encourages continuous contributions while deterring misuse or low-quality data submissions. This aligns with prior studies (e.g., Shinde et al., 2020) that argue incentives are crucial for maintaining an active and reliable CTI network.

From a technical perspective, the choice of a consortium blockchain, as opposed to public or fully private chains, strikes a practical compromise between scalability, trust boundaries, and regulatory compliance. In a consortium model, only vetted entities participate in the consensus process, which increases transaction throughput while maintaining a high level of security and auditability. This design is especially suitable for cross-sector cybersecurity alliances, where governance and accountability must be tightly controlled.

Finally, the framework aligns with established cybersecurity governance principles, such as the NIST Cybersecurity Framework, ISO/IEC 27010 for inter-organizational information exchange, and the MITRE ATT&CK model for threat behaviour classification. This ensures that the model is not only theoretically sound but also compatible with real-world implementation environments.

Nevertheless, while the conceptual model offers a strong theoretical foundation, its effectiveness remains to be empirically validated. Potential challenges, such as interoperability with legacy systems, regulatory heterogeneity across regions, and the technical complexity of blockchain integration, must be carefully addressed in future work. Additionally, the governance structure for managing access rights, onboarding participants, and handling malicious actors needs to be clearly defined and evaluated in operational settings.

VI. CONCLUSION AND FUTURE WORK

A. *Conclusion*

This paper develops a blockchain-based conceptual system to enable secure and reliable CTI information sharing. Through its design, this model solves enduring sharing system problems related to trust issues and data security and participation motivation. Through the implementation of smart contracts as well as access control mechanisms and decentralised governance, the conceptual framework creates a new approach which enhances threat visibility while enabling coordinated cyber defense activities. More validation through prototyping testing is essential to validate this work, but the study adds value to emerging technology-based cybersecurity collaboration research.

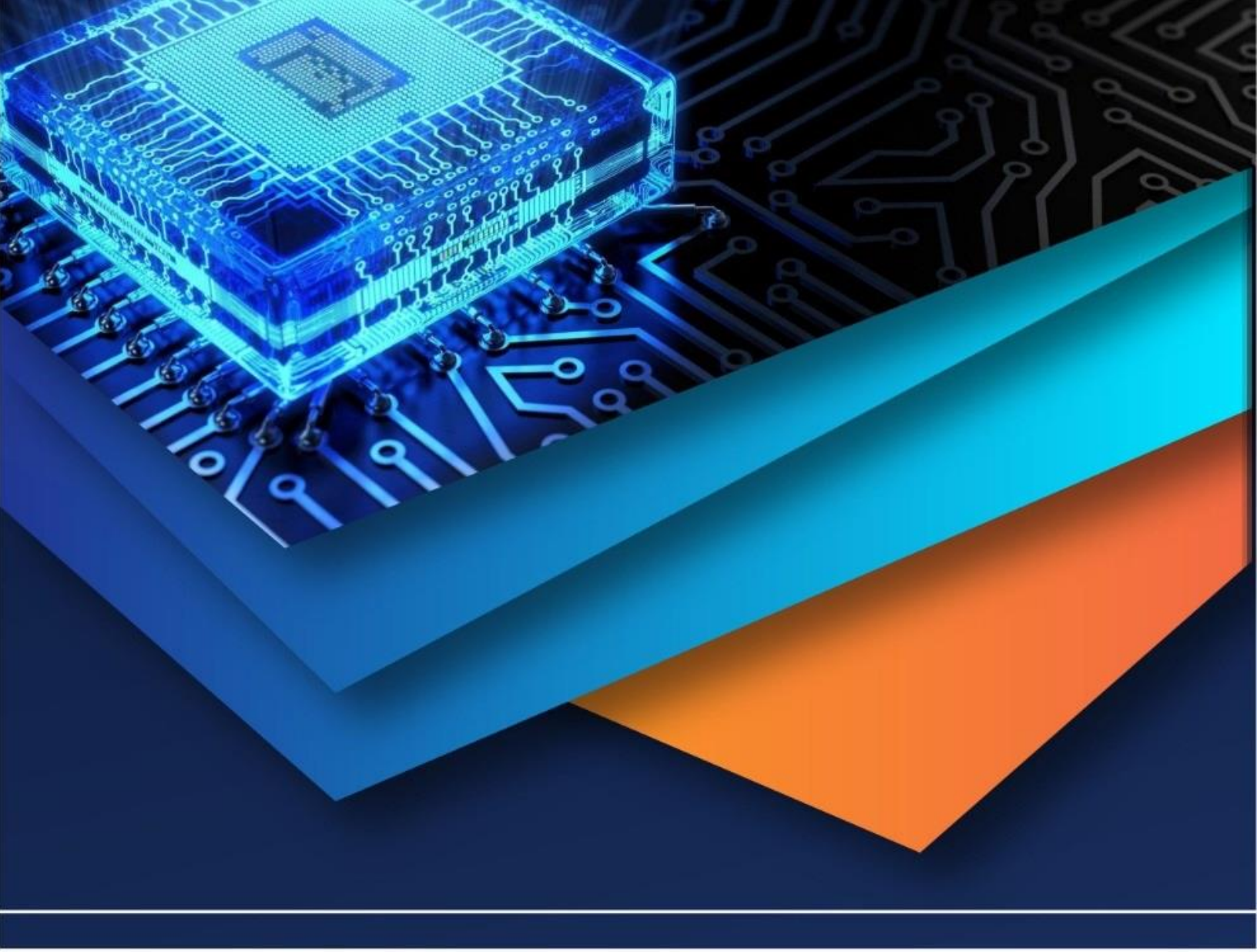
B. *Future Works*

This study is conceptual and does not present empirical data or a real-world implementation. Scalability, latency, and legal concerns remain open challenges, particularly when dealing with large volumes of threat intelligence and cross-border data sharing. Future work should focus on developing a working prototype to evaluate the model's performance in real-world scenarios. Further exploration of privacy-preserving techniques (e.g., homomorphic encryption, zero-knowledge proofs) and alignment with regulatory requirements will also be essential for practical adoption.

REFERENCES

[1] Ala'M, A. A., Alsmadi, I., & Alshawabkeh, M. (2021). Cyber threat intelligence: A comprehensive review of the current state and future directions. Computers & Security, 102, 102152. https://doi.org/10.1016/j.cose.2020.102152
[2] Shinde, S., Laborde, R., & Cavallaro, L. (2020). Incentivizing threat intelligence sharing: Challenges and opportunities. Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 96–104. https://doi.org/10.1109/EuroSPW51379.2020.00019
[3] Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. IEEE Access, 8, 16440–16455. https://doi.org/10.1109/ACCESS.2020.2967218
[4] Undercoffer, J., & Joshi, A. (2019). Blockchain-enabled cyber threat intelligence sharing system. In Blockchain and Cybersecurity (pp. 103–123). Springer.
[5] Stojanovic, L., Milinkovic, D., & Kelemen, M. (2021). Blockchain-based solutions for enhancing cyber threat intelligence exchange. In Future Generation Computer Systems, 115, 280–293. https://doi.org/10.1016/j.future.2020.09.016
[6] MITRE Corporation. (2023). MITRE ATT&CK® Framework. https://attack.mitre.org/
[7] OASIS. (2022). STIX™ Version 2.1 and TAXII™ Version 2.1 Specifications. https://oasis-open.github.io/cti-documentation/
[8] National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[9] ISO/IEC 27010:2015. (2015). Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications. International Organization for Standardization.
[10] Buterin, V. (2016). The blockchain trilemma: Decentralization, security, and scalability. Ethereum Foundation.
[11] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[12] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). https://doi.org/10.1109/SPW.2015.27
[13] Cheng, Y., Liu, Z., Wang, C., & Zhou, H. (2020). CyberChain: A blockchain-based data sharing system for cybersecurity information. Future Internet, 12(11), 184.
[14] Ma, Z., Wang, Q., Ma, L., & Yu, W. (2021). Blockchain-Based Intelligence Sharing for Malware Threats. IEEE Transactions on Network and Service Management, 18(2), 1541–1555.
[15] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72, 212–233.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY