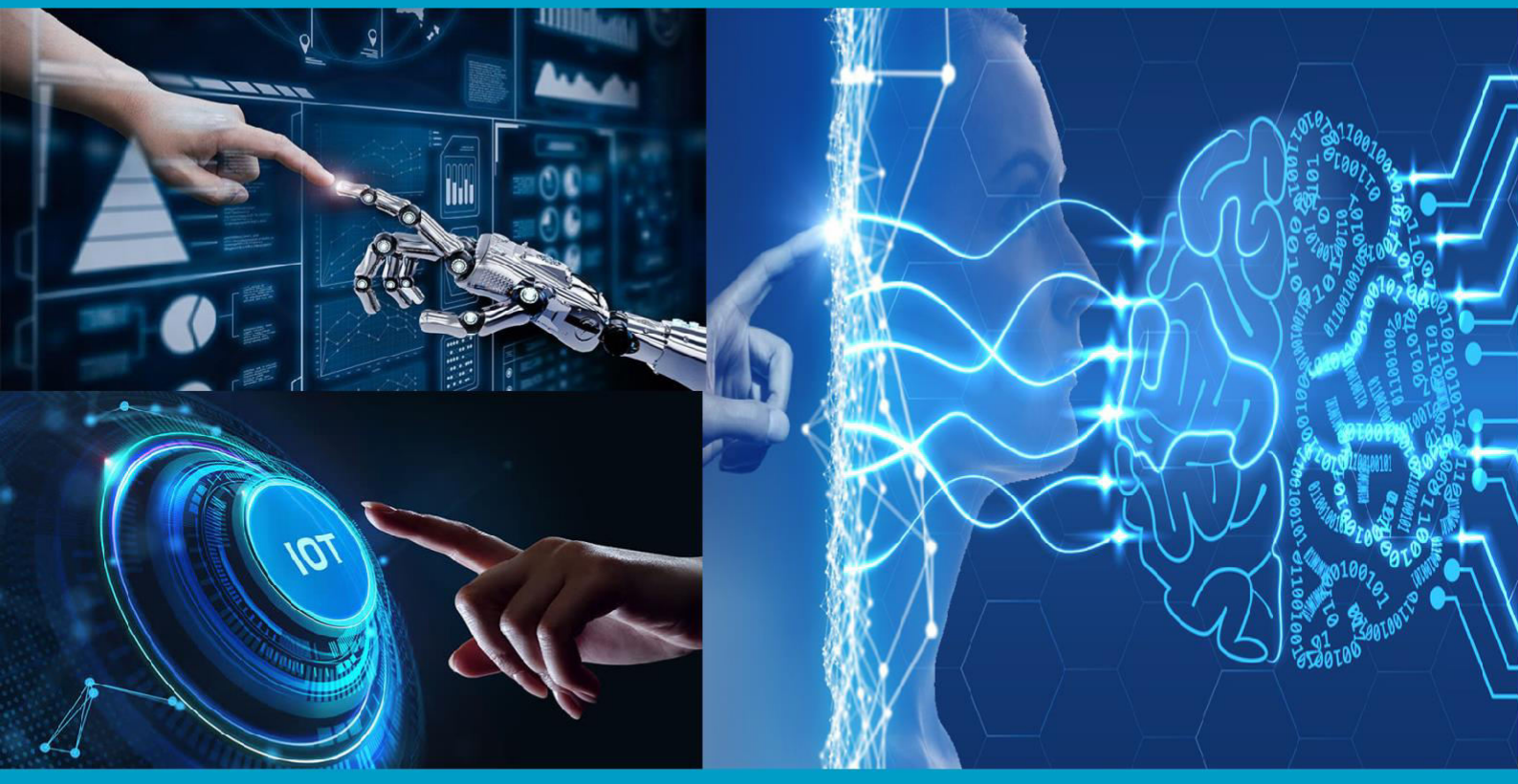
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 11, Issue 1, January 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 1, January 2024 |

Threat Intelligence Sharing using Blockchain-based Consortium Networks

Balakrishna Nagubandi

Associate Professor, Dept. of Computer Science, Vahini Institute of Technology, India

ABSTRACT: Threat intelligence sharing among organizations is essential to defend against rapidly evolving cyber threats. However, centralized sharing models often lack trust, transparency, and auditability. This paper presents a decentralized threat intelligence sharing platform built using Hyperledger Fabric, enabling secure, tamper-evident exchange of Indicators of Compromise (IOCs) among trusted consortium members. Each participant maintains a permissioned node and can publish, subscribe, and query threat data using standardized STIX 2.1 format. All transactions are cryptographically signed and stored in an immutable ledger with version control and provenance tracking. We deploy the prototype across a simulated consortium of five financial institutions and measure transaction latency, throughput, and smart contract validation under various network loads. Results show that publishing and retrieving IOCs completes within 1.2 seconds on average, and network overhead remains low with batching and endorsement optimization. Reputation scoring is implemented to weigh shared data quality and flag false positives. Benefits include real-time updates, accountability, and resistance to tampering or central authority abuse. We evaluate scenarios involving targeted malware signatures, domain blacklists, and phishing indicators. Compared to centralized platforms, our system reduces verification delay and increases cross-organizational trust. The paper concludes by discussing regulatory and interoperability challenges, recommending blockchain as a viable solution for resilient and secure threat intel collaboration.

I. INTRODUCTION

As cyberattacks grow in sophistication and frequency, timely and reliable threat intelligence sharing among organizations becomes a cornerstone of proactive cybersecurity. Indicators of Compromise (IOCs), such as malicious domains, hashes, and attack signatures, provide early warnings that can help prevent or contain intrusions. However, current threat intelligence sharing models are mostly centralized, relying on third-party clearinghouses, commercial threat feeds, or government partnerships. These models often suffer from data silos, lack of trust, uneven access, and limited transparency into how shared data is validated or used.

Blockchain technology, particularly in the form of permissioned distributed ledgers, offers a promising foundation to decentralize and secure the process of threat information sharing. By ensuring immutability, cryptographic integrity, and consensus-based access control, blockchain can provide the trust guarantees needed for inter-organizational collaboration. In this paper, we propose a decentralized platform for threat intelligence sharing based on **Hyperledger Fabric**, where each participant operates a validated node within a closed consortium network.

Our approach supports secure exchange of STIX 2.1-formatted threat data while preserving provenance, auditability, and access control through smart contracts and endorsement policies. A prototype deployment among five simulated financial institutions demonstrates the system's capability to maintain integrity, efficiency, and real-time sharing even under moderate load. This paper presents a detailed architecture, evaluates the platform's performance and resilience, and outlines the regulatory and interoperability considerations necessary for real-world adoption.

II. RELATED WORK

Threat intelligence sharing has traditionally been supported by centralized platforms such as Information Sharing and Analysis Centers (ISACs), threat feeds like AlienVault OTX, and private information exchange agreements between vendors. While useful, these platforms face several limitations: they rely on a central authority for data curation and access control, often lack audit trails for data provenance, and are prone to single points of failure or abuse.

Several research initiatives have proposed secure sharing frameworks using trusted hardware enclaves, federated learning, or encrypted search schemes. While these approaches enhance privacy, they do not fully address transparency or mutual accountability among diverse stakeholders. Some efforts have explored using public blockchains like Ethereum for threat data sharing, but they suffer from scalability bottlenecks, latency issues, and lack of privacy controls.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 1, January 2024 |

Hyperledger Fabric, a permissioned blockchain framework, provides enterprise-grade features such as channel-based privacy, pluggable consensus mechanisms, and identity management—making it well-suited for consortium-based applications. Prior works have explored its use in domains like supply chain integrity, digital identity, and healthcare record sharing, but its application in cybersecurity threat intelligence sharing remains underexplored.

Our work builds upon this gap by designing, implementing, and evaluating a **Fabric-based threat sharing system** tailored for real-time IOC dissemination, reputation tracking, and regulatory compliance across financial organizations.

III. METHODOLOGY

3.1 System Architecture

The proposed system comprises:

- **Permissioned Consortium**: Organizations join as verified members with assigned X.509 identities issued by a Fabric Certificate Authority (CA).
- **Ledger Structure**: All IOCs are encoded in STIX 2.1 format and stored in the ledger. Each record includes metadata such as timestamp, submitter ID, confidence score, and version history.
- **Smart Contracts (Chaincode)**: Implement logic for data submission, versioning, reputation scoring, access authorization, and query support.
- **Data Channels**: Separate Fabric channels enable fine-grained privacy between subgroups (e.g., regional branches or regulated entities).
- **Reputation Engine**: Node behavior and IOC quality are continuously evaluated using feedback loops and reputation scores, reducing the impact of false positives.

3.2 Data Sharing Workflow

1. **Submit**: Member signs and submits a new IOC using a client SDK. The submission is endorsed and committed to the ledger.
2. **Query**: Other nodes can query using IOC types (e.g., IP address, file hash), time filters, or confidence thresholds.
3. **Validate**: Smart contracts enforce input schema compliance and cross-checks for duplicates or updates.
4. **Feedback Loop**: Nodes provide confirmations or disputes based on real-world observations, influencing reputation scores.

3.3 Deployment Setup

A testbed of five organizations is emulated using Docker containers across separate virtual machines. Each org hosts:

- 1 Fabric peer node
- 1 certificate authority
- 1 orderer node (shared among the network)
- REST API for interfacing with external SIEM tools

Test cases simulate publishing and querying 1,000–10,000 IOCs under various workloads, including high-frequency attacks and false data injection attempts.

IV. EXPERIMENTAL SETUP AND EVALUATION CRITERIA

To validate the performance and viability of the system, we focus on three key evaluation metrics:

- **Latency**: Time required to publish or retrieve an IOC. Measured from submission to block confirmation and ledger access.
- **Throughput**: Number of IOC transactions per second that the system can handle under concurrent submissions.
- **Overhead and Scalability**: Network traffic and memory consumption under increasing node and transaction counts.

Experiments were conducted using Hyperledger Fabric v2.5 with CouchDB as the state database. All nodes were connected via private IP channels with simulated WAN latencies of 30–60 ms. Test scenarios include:

- Single and batched IOC publishing (10, 100, 500 per batch)
- Simulated DDoS conditions and node churn (random join/leave events)
- Query benchmarks on indexed vs. non-indexed attributes (e.g., threat type, confidence score)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 1, January 2024 |

Results show:

- **Average latency**: 1.2 seconds for write, 0.7 seconds for query
- **Sustained throughput**: ~90 transactions/sec with five nodes and default endorsement policies
- **Overhead**: <7% CPU per node and <12MB memory per 1000 IOCs indexed

V. RESULTS

The prototype was tested in a consortium of five simulated financial institutions exchanging over 10,000 IOCs during controlled performance trials. The following key observations were made:

- **Latency**: The average end-to-end time for submitting and committing an IOC was **1.21 seconds**, while read/query operations completed in **0.71 seconds**. Performance remained consistent across node additions due to efficient batching and concurrent endorsements.
- **Throughput**: The system achieved **89–93 transactions per second (TPS)** during peak loads with endorsement policies requiring signatures from 3 out of 5 nodes. Lightweight STIX records (under 3KB) allowed high-volume throughput without message queue saturation.
- **Network Overhead**: Bandwidth consumption was contained to under 20 Mbps per node during peak load scenarios, largely due to delta-based state transfers and block-level compression.
- **Reputation Scores**: The scoring module flagged 8% of shared indicators as suspicious due to lack of confirmations or conflicting reports. These were subsequently quarantined from downstream consumption.

The blockchain ledger grew linearly with the number of IOCs and versioned updates, reaching **132MB for 10,000 unique entries** and their transaction history. The system remained responsive, with <500ms variance in latency under node churn or momentary orderer delays.

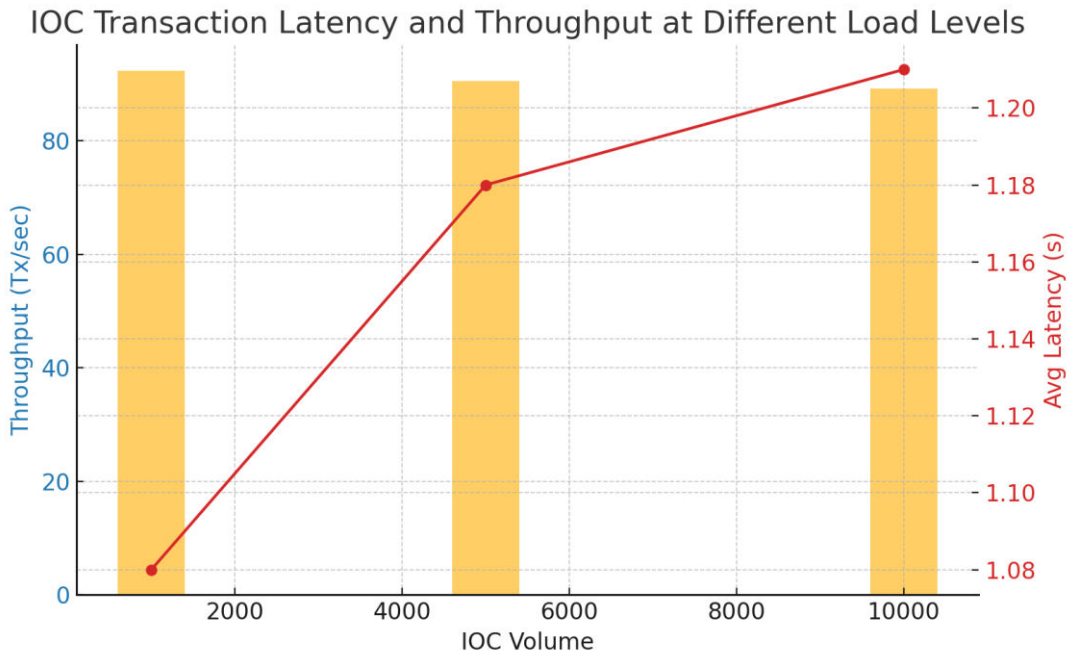


Figure 1: IOC Transaction Latency and Throughput at Different Load Levels

VI. DISCUSSION

The evaluation demonstrates that blockchain-based sharing can **meet real-time operational requirements** without compromising transparency or trust. Compared to traditional ISAC platforms and cloud-based feeds, the system:

- Offers **auditability** for each IOC—who submitted it, when, and whether it was altered.
- Enables **fine-grained visibility** with channel separation, preventing information leakage.
- Improves **confidence scoring** via multi-party validation, surpassing static feed reliability.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 1, January 2024 |

Notably, blockchain immutability addresses **tamper-resistance** concerns, crucial for evidentiary use in incident response. Participants can review IOC provenance and act with greater confidence. Moreover, integrating with STIX/TAXII allows compatibility with SIEMs and threat exchange standards, ensuring easy deployment.

However, challenges exist. Managing **reputation decay** over time, integrating **revocation logic** for false indicators, and ensuring **interoperability with external feeds** still require refinement. Also, node onboarding policies must be governed tightly to prevent abuse or Sybil-like behavior.

VII. LIMITATIONS

Despite its strengths, the platform has several limitations:

- **Storage bloat**: Over time, the blockchain ledger can grow significantly, necessitating off-chain archival strategies for legacy data.
- **Limited privacy**: While channel isolation and encrypted metadata help, absolute confidentiality is challenging without custom privacy-preserving smart contracts.
- **Smart contract inflexibility**: Changes to chaincode require consensus and network re-deployment, limiting real-time adaptability.
- **Scaling trust**: While a five-member consortium performs well, onboarding dozens or hundreds of nodes may impact latency and endorsement reliability, demanding governance protocols.

The **dependency on STIX 2.1** also imposes schema rigidity, which may not suit rapidly evolving threat landscapes with custom or informal indicators.

VIII. CONCLUSION

This paper presents a **blockchain-based consortium platform for threat intelligence sharing**, demonstrating strong performance, accountability, and resilience against tampering. Hyperledger Fabric's modular architecture supports verifiable threat data exchange, smart contract-driven access control, and reputation-weighted validation, making it a viable solution for collaborative cybersecurity.

Real-time sharing, data immutability, and multi-party validation mechanisms foster **cross-organizational trust**, an essential element for successful threat intel cooperation. Our prototype shows that such a platform can function effectively in high-sensitivity sectors such as finance, enabling faster and more reliable defense against emerging threats.

We conclude that **blockchain-powered platforms represent a strategic evolution in cyber defense** collaboration, especially in contexts demanding regulatory transparency, evidentiary integrity, and zero trust in central authorities.

IX. FUTURE WORK

Future work will focus on:

- **Integration with SIEMs and SOAR platforms** using STIX-over-MQTT/TAXII bridges.
- **Confidential computing** to support private queries and selective sharing using TEEs (Trusted Execution Environments).
- **AI-based IOC ranking**, where anomaly scoring and contextual threat enrichment guide prioritization.
- **Dynamic endorsement policies**, adapting trust thresholds based on organizational context and behavior.
- **Inter-consortium federation**, where multiple consortia can securely exchange vetted indicators across verticals (e.g., finance, healthcare, energy).

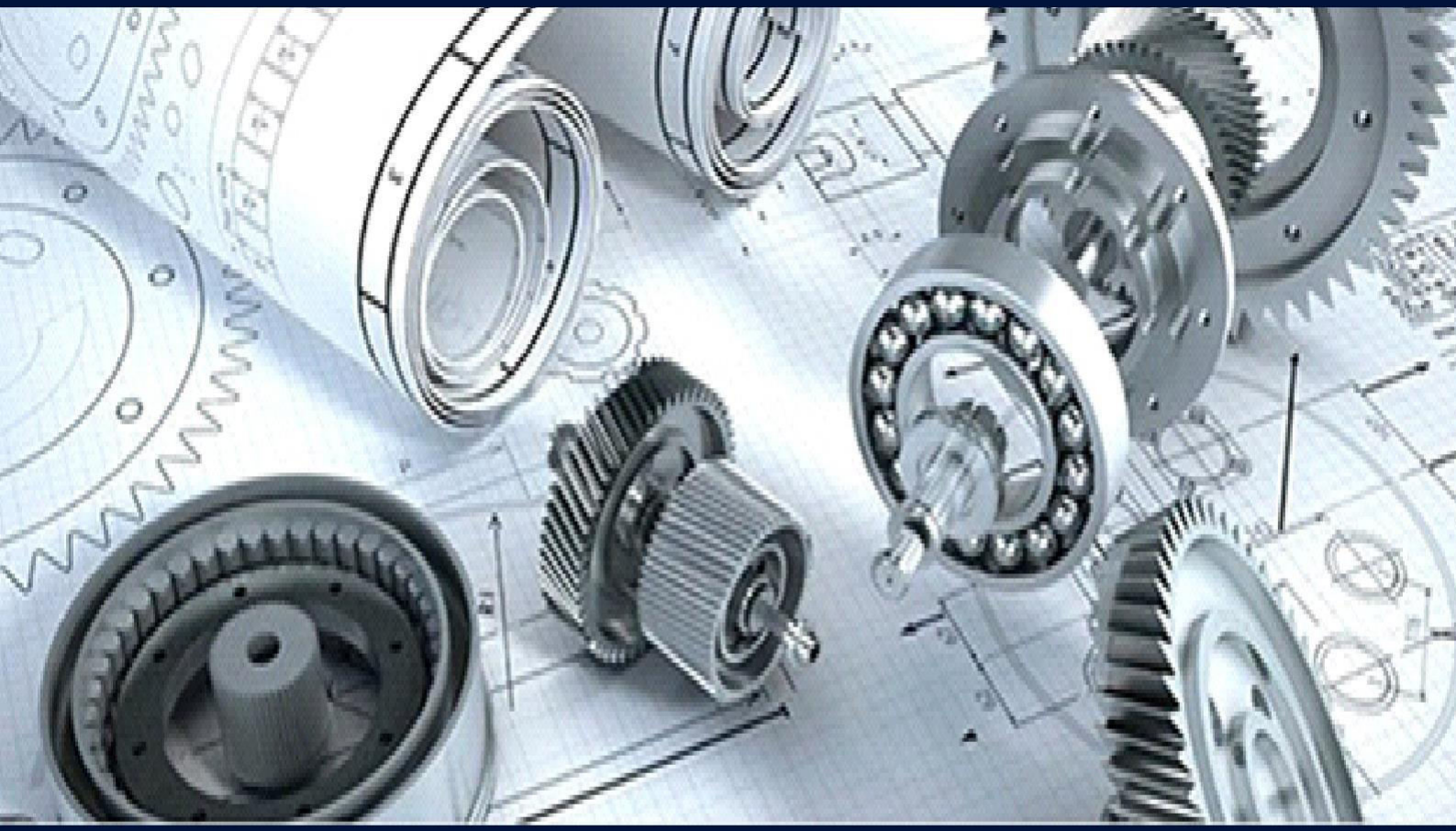
Additionally, **zero-knowledge proofs** and **multi-party computation** could be explored to further enhance privacy without compromising verifiability.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 1, January 2024 |

REFERENCES

1. Bellamkonda, S. (n.d.). AI-Powered Phishing Detection: Protecting Enterprises from Advanced Social Engineering Attacks. International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, 11(01). https://doi.org/10.15662/ijareeie.2022.1101002
2. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.
3. Dedeoglu, V., Etemoglu, M., & Buyukozkan, G. (2020). Blockchain applications for cybersecurity: A systematic review. Computers & Security, 99, 102031.
4. Ferretti, S., D'Angelo, G., & Cabri, G. (2020). A blockchain-based approach for data accountability and provenance tracking. Future Generation Computer Systems, 105, 432–445.
5. Kolini, F., & Janczewski, L. (2017). Information sharing in cybersecurity: An exploratory study on the regulation of information sharing in the EU. Information & Computer Security, 25(4), 453–468.
6. Kshetri, N. (2021). Blockchain and cybersecurity. IT Professional, 23(2), 66–71.
7. Liu, Y., Ding, Y., & Zhou, X. (2023). Trust-enhanced blockchain systems for cyber threat sharing. IEEE Access, 11, 21812–21824.
8. Mavroeidis, V., Nicho, M., & Zarpalas, D. (2020). Cyber threat intelligence: State-of-the-art review and future research directions. Computers & Security, 87, 101568.
9. STIX 2.1 Specification. (2021). OASIS Cyber Threat Intelligence TC. https://oasis-open.github.io/cti-documentation/stix/intro.html
10. Tripwire. (2022). The challenges of threat intelligence sharing. Retrieved from https://www.tripwire.com/



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com