Federated and Collaborative Cyber Threat Intelligence (CTI) Sharing Frameworks

Aarav Tyagi[1], Sita N. Rao[2], Ishaan Verma[3]
Lecturer[1], Students[2, 3]
Department of CSE
Velagapudi Ramakrishna Siddhartha Engineering College
Email ID: *Aaravtyagi45@gmail.com[1], sita_n5_rao@yahoo.com[2], ishaankkverma@rediffmail.com[3]*

ABSTRACT

Cyber threats have grown in complexity, scale, and coordination over the last decade. Traditional centralized Cyber Threat Intelligence (CTI) sharing models face challenges related to privacy, trust, scalability, and legal compliance. As organizations become increasingly interconnected, there is a strong need for collaborative yet privacy-preserving intelligence exchange mechanisms. Federated and collaborative CTI sharing frameworks have emerged as promising approaches that enable distributed entities to share threat insights without exposing sensitive internal data. These frameworks combine federated learning, secure multiparty computation, blockchain-based trust models, and standardized threat formats such as STIX and TAXII.

This paper provides a comprehensive review of federated and collaborative CTI sharing architectures, key enabling technologies, implementation models, benefits, and limitations. It also discusses trust establishment mechanisms, privacy preservation strategies, and real-world adoption challenges. A comparative analysis of centralized and federated CTI models is presented along with a conceptual architectural framework. The study concludes by identifying open research directions such as incentive mechanisms, adversarial robustness, and AI-driven automated intelligence validation.

KEYWORDS: *Cyber Threat Intelligence (CTI), Federated Learning, Collaborative Security, Threat Sharing, Blockchain Security, Privacy*

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

Preservation, Secure Multiparty Computation, STIX/TAXII

INTRODUCTION

Cyber Threat Intelligence (CTI) refers to the collection, analysis, and sharing of information related to cyber threats, vulnerabilities, indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs). In modern digital ecosystems, isolated security defenses are no longer sufficient. Attack campaigns often target multiple organizations simultaneously, making collaboration necessary.

Traditional CTI sharing platforms are usually centralized. Organizations submit intelligence to a trusted third party or Information Sharing and Analysis Center (ISAC). While effective in some sectors, this model introduces several concerns:

- Data privacy risks
- Single point of failure
- Lack of trust between participants
- Regulatory restrictions (e.g., GDPR)
- Data ownership concerns

To overcome these limitations, federated and collaborative CTI frameworks have gained research interest. These approaches allow organizations to collaborate without directly sharing raw sensitive data. Instead, they share aggregated insights, trained models, or encrypted indicators.

The rest of this paper reviews the core concepts, technologies, architectures, and challenges of such frameworks.

BACKGROUND ON CYBER THREAT INTELLIGENCE SHARING

Cyber Threat Intelligence (CTI) sharing has become a fundamental component of modern cybersecurity strategy. As attack, campaigns increasingly target multiple organizations simultaneously, sharing intelligence helps defenders move from reactive to proactive security posture. However, CTI is not uniform in nature. It exists at multiple abstraction levels, each serving different stakeholders and decision-making processes.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

1. Levels of Cyber Threat Intelligence

CTI sharing can occur at four primary levels: strategic, operational, tactical, and technical. Each level differs in audience, detail, and practical use.

a) Strategic Intelligence

Strategic intelligence focuses on high-level analysis of cyber threats. It is typically used by executive leadership, policy makers, and risk management teams. This level of intelligence answers questions such as:

- Who are the major threat actors targeting our sector?
- What geopolitical trends are influencing cyber operations?
- Which industries are being most affected by ransomware?
- What are the long-term risks to national or organizational security?

Strategic CTI often includes reports on advanced persistent threat (APT) groups, nation-state campaigns, cybercrime syndicates, and emerging global attack trends. It may discuss motivations, funding patterns, and regional risk factors. Unlike tactical data, strategic intelligence is less technical and more contextual.

For example, a strategic report may indicate that ransomware groups are increasingly targeting healthcare systems in developing countries due to weaker infrastructure. Such insights guide investment decisions, policy changes, and high-level security planning.

b) Operational Intelligence

Operational intelligence provides detailed insights into specific attack campaigns. It focuses on how a threat actor conducts operations, including:

- Attack timelines
- Command-and-control (C2) infrastructure
- Phishing campaign details
- Exploited vulnerabilities
- Tools and malware families used

This level of CTI is highly valuable for security operations centers (SOCs) and incident response teams. It helps organizations understand the lifecycle of an attack and anticipate next steps.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

For instance, operational intelligence may reveal that a ransomware campaign first uses spear-phishing emails, followed by credential harvesting, lateral movement via PowerShell scripts, and final payload deployment through a remote access tool. Such information allows defenders to deploy targeted monitoring and early detection strategies.

Operational intelligence bridges the gap between strategic insights and actionable technical indicators.

c) Tactical Intelligence

Tactical intelligence is more granular and machine-readable. It typically includes Indicators of

Compromise (IoCs), such as:

- Malicious IP addresses
- Domain names
- File hashes (MD5, SHA-256)
- Email headers
- URLs
- Registry keys

These indicators are directly consumed by intrusion detection systems (IDS), firewalls, endpoint detection and response (EDR) tools, and SIEM platforms.

Tactical CTI is often shared in near real-time to block ongoing threats. However, it has limitations. Indicators can quickly become outdated because attackers frequently rotate IP addresses and domains. Therefore, while tactical intelligence is useful for immediate defense, it requires constant updating.

d) Technical Intelligence

Technical intelligence refers to deep forensic and malware-level details. It includes:

- Reverse-engineered malware code
- Binary signatures
- Exploit kits
- Vulnerability details (CVE information)

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

- Packet capture (PCAP) data
- System logs and memory dumps

This type of intelligence is primarily used by malware analysts, digital forensics experts, and advanced research teams. It helps in understanding the internal workings of malicious tools and discovering detection signatures.

Technical intelligence is highly sensitive because it may expose internal infrastructure or investigative methods. Therefore, organizations are often reluctant to share it openly.

2. Existing Standards for CTI Sharing

Interoperability is a major challenge in CTI sharing. Different organizations use diverse security tools, logging systems, and data formats. To address this, standardized frameworks have been developed to ensure structured, machine-readable intelligence exchange.

a) STIX (Structured Threat Information Expression)

STIX is a standardized language used to represent cyber threat information in a structured format. It allows organizations to describe:

- Threat actors
- Attack patterns
- Campaigns
- Malware
- Vulnerabilities
- Relationships between entities

STIX uses JSON-based schemas and defines relationships such as “uses,” “targets,” or “attributed-to.” This relational structure enables complex threat modeling.

For example, a STIX object can represent a malware family linked to a specific threat actor and associated campaign. This makes CTI more contextual rather than just a list of isolated indicators.

b) TAXII (Trusted Automated Exchange of Intelligence Information)

TAXII is a transport protocol used to exchange STIX-formatted intelligence over secure

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

channels. It defines how CTI data is requested, shared, and synchronized between organizations.

Key features include:

- Secure HTTPS-based communication
- Authentication and authorization mechanisms
- Collection-based data sharing
- Push and pull models for intelligence distribution

TAXII enables automated and near real-time sharing between platforms, reducing manual intervention.

c) OpenIOC

OpenIOC (Open Indicators of Compromise) is an earlier format developed to standardize the sharing of forensic artifacts and indicators. It focuses on structured description of technical indicators such as registry keys, files, and processes.

Although less expressive than STIX, OpenIOC played an important role in early CTI automation. Some organizations still use it in forensic workflows.

Limitations of Existing Standards

While STIX, TAXII, and OpenIOC significantly improve machine-to-machine communication, they do not address core collaborative challenges such as:

- Trust between participating entities
- Data ownership concerns
- Privacy protection
- Incentive for contribution
- Verification of authenticity

Standards define “how to format and transmit data,” but they do not solve “whether participants are willing to share” or “how to ensure shared data is accurate and non-malicious.”

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

3. Limitations of Centralized CTI Platforms

Many CTI sharing systems rely on centralized architectures, such as national CERTs, ISACs, or vendor-managed platforms. Although these systems have facilitated collaboration, they present several structural limitations.

a) Single Point of Failure

Centralized systems depend on a trusted authority. If the central server is compromised, attacked, or misconfigured, the entire intelligence network may be disrupted. This increases systemic risk.

b) Trust Deficit

Organizations may hesitate to share sensitive information with a central authority due to concerns about:

- Data misuse
- Competitive disadvantage
- Exposure of internal weaknesses
- Government surveillance

Without strong trust, participation levels remain low.

c) Privacy and Regulatory Constraints

Laws such as GDPR, HIPAA, and data localization regulations restrict sharing of personal or sensitive data across borders. Raw logs may contain personal identifiers, making centralized sharing legally complex.

d) Information Overload

Central repositories often collect large volumes of indicators. Without proper validation mechanisms, they may include:

- False positives
- Outdated IoCs
- Duplicate entries
- Low-confidence intelligence

Security teams can become overwhelmed, reducing effectiveness.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

e) Lack of Incentive Mechanisms

Many organizations consume shared intelligence but contribute little in return. This "free-rider" problem weakens collaborative ecosystems.

Issue	Description	Impact
Trust Deficit	Organizations reluctant to share sensitive logs	Reduced participation
Privacy Concerns	Exposure of internal infrastructure data	Regulatory risks
Central Authority Dependence	Single control entity	Possible bias or breach
Scalability	High storage and computation overhead	Performance bottlenecks
Data Quality	False or outdated intelligence	Security gaps

FEDERATED CTI SHARING FRAMEWORKS

Federated CTI frameworks apply principles of federated learning (FL) and distributed computing to threat intelligence collaboration.

1. Concept of Federated Learning in CTI

Federated learning allows multiple organizations to collaboratively train machine learning models without sharing raw data. Instead:

- Each organization trains a local model on its private threat data.
- Model updates (not raw data) are shared.
- A central aggregator combines updates to produce a global model.

This model can detect malware patterns, intrusion behaviors, or anomaly signatures across sectors.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

2. Architectural Model

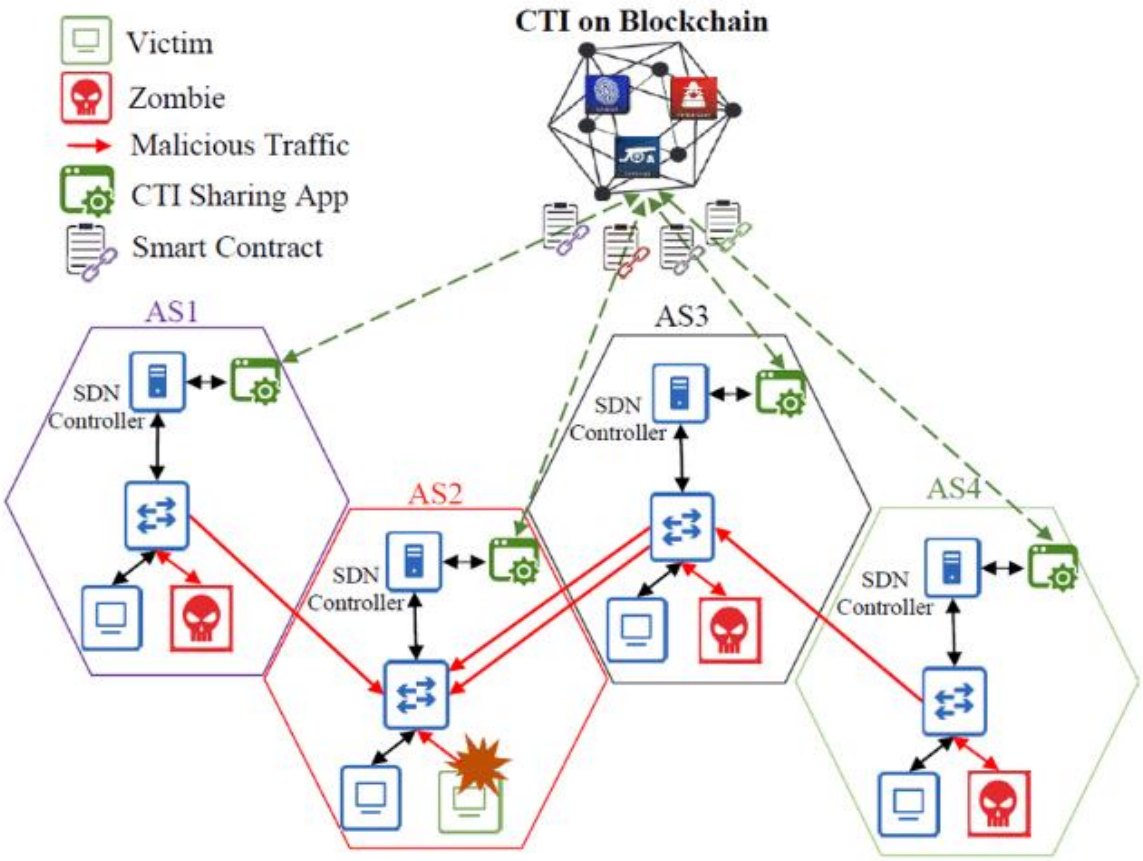


Figure 1: Federated CTI Sharing Architecture

3. Advantages

- Privacy preservation
- Improved detection accuracy
- Sector-wide collaboration
- Regulatory compliance support

4. Limitations

- Model poisoning attacks
- Communication overhead
- Heterogeneous data formats
- Unequal participation (stragglers problem)

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

COLLABORATIVE CTI SHARING MECHANISMS

Collaborative CTI frameworks extend beyond federated learning. They involve coordinated sharing mechanisms supported by trust technologies.

1. Blockchain-Based CTI Sharing

Blockchain offers:

- Immutable logging of threat submissions
- Transparent validation
- Decentralized governance
- Smart contract-based access control

Threat indicators can be hashed and recorded on-chain while actual data remains off-chain.

2. Secure Multiparty Computation (SMPC)

SMPC allows parties to jointly compute threat metrics without revealing their inputs. For example:

- Collaborative detection of botnet IP overlaps
- Shared anomaly scoring
- Risk correlation across networks

3. Differential Privacy

Differential privacy adds statistical noise to shared intelligence. It protects sensitive infrastructure details while preserving aggregate patterns.

4. Trust and Reputation Models

In collaborative environments, participants may provide false intelligence. Reputation scoring systems evaluate:

- Accuracy of previous submissions
- Validation frequency
- Community feedback

Such mechanisms encourage reliable contributions.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

COMPARATIVE ANALYSIS: CENTRALIZED VS FEDERATED CTI

Feature	Centralized Model	Federated Model
Data Sharing	Raw data often shared	Only model updates shared
Privacy	Lower	Higher
Scalability	Limited by central server	Distributed scalability
Trust	Depends on authority	Distributed trust
Regulatory Compliance	Challenging	Easier alignment
Attack Surface	Single point of failure	Distributed risk

Federated models offer stronger privacy but introduce complexity in coordination and aggregation.

IMPLEMENTATION CHALLENGES

1. Data Heterogeneity

Organizations use different logging formats, SIEM tools, and detection policies. Standardization is difficult.

2. Adversarial Attacks

Malicious participants may inject poisoned updates into federated learning systems. Robust aggregation algorithms such as Krum or Byzantine-resilient methods are required.

3. Incentive Mechanisms

Organizations often hesitate to contribute high-quality intelligence without clear benefits. Token-based or reputation-based incentives may encourage participation.

4. Legal and Regulatory Issues

Cross-border intelligence sharing may violate data localization laws. Privacy-preserving computation helps, but legal clarity is still required.

REAL-WORLD APPLICATIONS

1. Financial Sector

Banks collaborate to detect fraud campaigns and phishing infrastructures using federated anomaly detection models.

2. Healthcare Sector

Hospitals share ransomware detection models without exposing patient data.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

3. Critical Infrastructure

Energy and transportation networks use collaborative CTI to detect coordinated attacks on operational technology systems.

PROPOSED HYBRID FEDERATED-COLLABORATIVE FRAMEWORK

A hybrid framework can integrate:

- Federated Learning for AI-based detection
- Blockchain for trust and logging
- SMPC for secure metric computation
- STIX/TAXII for standardized exchange

Layered Architecture

- **Data Layer** – Local logs and threat repositories
- **Computation Layer** – Local ML training and SMPC
- **Consensus Layer** – Blockchain validation
- **Application Layer** – Global intelligence dashboard

Such layered architecture improves interoperability and security.

FUTURE RESEARCH DIRECTIONS

1. Adversarially Robust Federated CTI

Developing secure aggregation resistant to poisoning and model inversion attacks.

2. Automated Intelligence Validation

Using AI to verify authenticity of shared threat indicators.

3. Incentive Engineering

Game-theoretic models for fair intelligence contribution.

4. Interoperability Standards

Enhanced integration between STIX/TAXII and federated systems.

5. Quantum-Safe Secure Sharing

Exploring post-quantum cryptography in collaborative CTI environments.

CONCLUSION

Federated and collaborative CTI sharing frameworks represent a significant evolution from traditional centralized intelligence platforms. As cyber threats become more coordinated and

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved

advanced, no organization can operate in isolation. However, privacy concerns, trust issues, and regulatory barriers limit open sharing.

Federated learning enables collective intelligence without direct exposure of raw data, while blockchain and secure multiparty computation enhance transparency and trust. Although implementation challenges such as adversarial manipulation and heterogeneity remain, ongoing research is improving robustness and scalability.

Future developments must focus on incentive mechanisms, cross-sector governance models, and automated intelligence validation systems. If carefully implemented, federated CTI frameworks can create resilient and cooperative cybersecurity ecosystems capable of responding to global threats more effectively.

REFERENCES

1. S. Mittal, P. K. Das, “Cyber Threat Intelligence: Challenges and Opportunities,” IEEE Security & Privacy, 2020.
2. H. Takabi, J. Joshi, “Information Sharing in Cybersecurity: Models and Challenges,” ACM Computing Surveys, 2019.
3. I. Goodfellow et al., “Federated Learning for Distributed Security Analytics,” Journal of ML Security, 2021.
4. R. Roman, J. Lopez, “Distributed Trust Management in Cybersecurity,” Computer Networks, 2018.
5. NIST, “Guide to Cyber Threat Information Sharing,” Special Publication 800-150, 2016.
6. OASIS, “STIX Version 2.1 Documentation,” 2021.
7. OASIS, “TAXII Version 2.1 Specification,” 2021.
8. K. Bonawitz et al., “Secure Aggregation for Federated Learning,” CCS Proceedings, 2017.
9. M. Conti, A. Dehghantanha, “Blockchain for Cybersecurity and Threat Intelligence,” Future Generation Computer Systems, 2020.
10. Y. Liu et al., “Adversarial Attacks in Federated Learning,” IEEE Security & Privacy, 2020.

Page 159-171 © MANTECH PUBLICATIONS 2025. All Rights Reserved