International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 9, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i9.809

Confidential Computing Threat Exchange: Enabling Collective Defense Through Secure Cross-Sector Intelligence Sharing

Winifred Chukwuebuka Ayogu[1]

[1]Department of Cybersecurity and Networks, Tagliatela College of Engineering, University of New Haven, United States of America

Publication Date 2025/09/17

Abstract

The increasing sophistication of cyber threats necessitates unprecedented levels of collaboration across critical infrastructure sectors. This paper presents a comprehensive framework for confidential computing-enabled threat intelligence exchange that preserves privacy while enabling real-time collective defense capabilities. By leveraging secure enclaves, standardized threat indicator formats, and coordinated response protocols, organizations can share attested threat indicators without exposing sensitive operational data. Our analysis demonstrates how utilities, hospitals, banks, and ports can establish a national early-warning grid capable of detecting and mitigating coordinated attacks within minutes rather than hours or days.

Keywords: *Confidential Computing, Threat Intelligence Sharing, Secure Enclaves, STIX/TAXII, Critical Infrastructure Protection.*

I. INTRODUCTION

Modern cyber adversaries increasingly target multiple sectors simultaneously, exploiting interconnections between critical infrastructure systems to amplify their impact (Carter et al., 2024). Traditional threat intelligence sharing mechanisms often fail to provide timely, actionable intelligence due to privacy concerns, regulatory constraints, and technical limitations that prevent organizations from sharing detailed telemetry data (Harrison et al., 2022). This research gap has created vulnerabilities that sophisticated threat actors routinely exploit.

Confidential computing presents a paradigm shift in how organizations can collaborate on cybersecurity while maintaining data sovereignty and regulatory compliance (Russinovich, 2024). By utilizing hardware-based trusted execution environments, organizations can process and analyze threat data collectively without exposing proprietary information or violating privacy regulations. This approach enables the creation of a national early-warning system that can detect coordinated attacks across sectors in near real-time Adeshina, (2021).

The primary contribution of this paper is a comprehensive framework that integrates confidential computing technologies with established threat intelligence sharing protocols to create a secure, scalable, and effective cross-sector defense mechanism. We examine how secure enclaves can isolate threat analytics and encryption keys, how standardized indicator formats can normalize and route threat fingerprints, and how Information Sharing and Analysis Centers (ISACs) can coordinate responses without compromising operational security.

II. BACKGROUND AND LITERATURE REVIEW

- *Confidential Computing Foundations*

Confidential computing represents a fundamental advancement in protecting data during processing, complementing traditional encryption methods that secure data at rest and in transit (Li et al., 2024). The technology relies on hardware-based trusted execution environments (TEEs) that create isolated processing spaces, known as secure enclaves, where sensitive computations can occur without exposure to the underlying operating system or hypervisor Adeshina & Ndukwe, (2024).

Contemporary implementations utilize three primary hardware architectures: Intel Software Guard Extensions (SGX), AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP), and ARM Confidential Compute Architecture (CCA) (Yoon et al., 2022). Each technology provides unique capabilities for isolating workloads and protecting against different threat vectors, as detailed in Table 1.

Table 1 Comparison of Confidential Computing Technologies

Technology	Isolation Level	Memory Protection	Attestation Support	Performance Impact	Use Case Suitability
Intel SGX	Application-level	Hardware encryption	Remote attestation	5-15% overhead	Lightweight analytics
AMD SEV-SNP	VM-level	Memory encryption	Platform attestation	2-8% overhead	Full workload isolation
ARM CCA	Realm-level	Hardware isolation	Realm attestation	3-10% overhead	Cloud-native deployments

The evolution of confidential computing has been particularly significant in cloud environments, where the need to protect workloads from privileged access has become paramount (Kaplan, 2023). Recent developments in confidential GPUs have extended these protections to machine learning workloads, enabling privacy-preserving analytics at scale (Dhanuskodi et al., 2023).

- *Threat Intelligence Sharing Challenges*

Traditional cyber threat intelligence sharing faces numerous obstacles that limit its effectiveness in preventing large-scale attacks. Research by Tounsi and Rais (2018) identified key challenges including data quality inconsistencies, lack of standardization, and concerns about competitive disadvantage. These issues are compounded by regulatory requirements that often prohibit sharing of detailed network telemetry data across organizational boundaries.

The Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) standards have emerged as foundational protocols for threat intelligence sharing (Barnum, 2020). However, implementation challenges persist, particularly around maintaining data confidentiality while enabling meaningful analysis across organizational boundaries. Komarov et al. (2022) demonstrated how blockchain technologies could enhance security in TAXII implementations, though scalability concerns remain.

Information Sharing and Analysis Centers (ISACs) have played a crucial role in facilitating sector-specific threat intelligence sharing, yet their effectiveness is often limited by trust concerns and information asymmetries (Carrapico & Farrand, 2016). The benefits of information sharing, while significant, must be balanced against risks including potential exposure of sensitive operational details and the possibility of adversaries infiltrating sharing networks (Asghari et al., 2015).

- *Privacy-Preserving Security Analytics*

The intersection of privacy preservation and security analytics has received increasing attention as organizations seek to leverage collective intelligence while maintaining data protection (Lazouski et al., 2021). Traditional approaches often rely on data anonymization or aggregation techniques that reduce the utility of shared information for threat detection purposes.

Recent advances in secure multi-party computation and homomorphic encryption have shown promise for privacy-preserving threat detection, though computational overhead remains a significant barrier to real-time implementation (Sun et al., 2021). The integration of trusted execution environments with machine learning workflows has emerged as a particularly promising approach for maintaining both privacy and analytical utility (Alhajjar et al., 2021).

III. CONFIDENTIAL COMPUTING TECHNOLOGIES FOR THREAT INTELLIGENCE

- *Hardware-Based Trusted Execution Environments*

The foundation of confidential computing threat exchange lies in hardware-based trusted execution environments that provide cryptographic guarantees for data confidentiality and integrity during processing Yusuf, (2023). These technologies have evolved significantly since their initial introduction, with each generation addressing specific limitations in security, performance, and usability (Han et al., 2023).

Intel Software Guard Extensions (SGX) pioneered application-level confidential computing by creating secure enclaves within standard processor cores. SGX isolates sensitive code and data in memory regions that are encrypted and access-controlled by the processor hardware. For threat intelligence applications, SGX enables organizations to process threat indicators within enclaves while maintaining cryptographic assurance that neither the operating system nor hypervisor can access the raw data.

AMD's Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) takes a different approach by providing whole-system memory encryption at the virtual machine level. This technology is particularly well-suited for threat intelligence workloads that require full operating system environments or complex software stacks. SEV-SNP's ability to isolate entire virtual machines while

maintaining near-native performance makes it ideal for processing large volumes of threat telemetry across diverse analytical frameworks.

ARM's Confidential Compute Architecture (CCA) introduces a novel "realm" concept that provides isolation between workloads while enabling secure communication between realms. This architecture is particularly relevant for edge computing scenarios where threat intelligence must be processed at distributed locations with varying trust levels.

➢ *Remote Attestation and Trust Establishment*

A critical component of confidential computing threat exchange is the ability to establish trust in remote computing environments through cryptographic attestation (Delignat-Lavaud et al., 2023). Remote attestation enables organizations to verify that threat intelligence processing occurs within genuine secure enclaves running authorized software configurations.

The attestation process typically involves three phases: platform verification, software measurement, and policy validation. During platform verification, the requesting organization receives cryptographic proof that the remote system contains legitimate confidential computing hardware. Software measurement provides cryptographic hashes of the exact code running within the secure enclave, enabling verification that only authorized threat intelligence processing software is executing. Policy validation ensures that the enclave configuration meets organizational security requirements for data processing.

Table 2 Remote Attestation Capabilities by Platform

Platform	Attestation Method	Verification Scope	Trust Anchor	Typical Validation Time
Intel SGX	EPID/DCAP	Enclave + Platform	Intel PKI	100-500ms
AMD SEV-SNP	Platform Security Processor	VM + Platform	AMD ARK	200-800ms
ARM CCA	Realm Management Monitor	Realm + Platform	ARM PSA	150-600ms

This attestation framework enables the creation of federated threat intelligence networks where organizations can verify the security posture of remote processing environments before sharing sensitive indicators. The cryptographic nature of attestation provides non-repudiation guarantees that are essential for regulatory compliance and audit requirements.

➢ *Secure Key Management and Cryptographic Isolation*

Effective threat intelligence sharing requires sophisticated key management systems that can operate within the constraints of confidential computing environments while maintaining operational flexibility (Rüsch & Vigna, 2020). Traditional key management approaches often conflict with the isolation requirements of secure enclaves, necessitating new architectural patterns.

The proposed framework utilizes a hierarchical key derivation scheme where master keys are generated and stored exclusively within secure enclaves. These master keys are never exposed to conventional software environments, ensuring that even privileged system administrators cannot access the cryptographic material protecting shared threat intelligence.

Key rotation procedures are particularly critical in threat intelligence applications due to the sensitive nature of the data and the potential for long-term compromise of shared indicators. The framework implements automated key rotation with forward secrecy guarantees, ensuring that compromise of current cryptographic material cannot retroactively expose previously shared intelligence.

➢ *Performance Considerations and Optimization*

While confidential computing provides strong security guarantees, performance considerations are crucial for real-time threat intelligence processing (Khatoun & Khoukhi, 2022). The cryptographic operations required for memory encryption and attestation introduce computational overhead that can impact the responsiveness of threat detection systems.

Optimization strategies include selective use of confidential computing for the most sensitive analytical components while maintaining conventional processing for less sensitive operations. Machine learning model inference, for example, can be performed within secure enclaves while feature extraction and data preprocessing occur in standard environments with appropriate data transformation to preserve privacy.

Memory management within secure enclaves requires careful consideration due to the limited enclave page cache (EPC) available in current SGX implementations and similar constraints in other platforms. Efficient memory allocation and garbage collection strategies are essential for maintaining high throughput in threat intelligence processing pipelines.

IV. SECURE THREAT INTELLIGENCE EXCHANGE ARCHITECTURE

➢ *Federated Enclave Networks*

The architecture for confidential computing threat exchange relies on federated networks of secure enclaves distributed across participating organizations. This design enables collective threat analysis while maintaining organizational autonomy and data sovereignty. Each participating organization operates one or more secure enclaves configured for specific threat intelligence functions, creating a distributed processing fabric that can scale to accommodate varying workload demands.

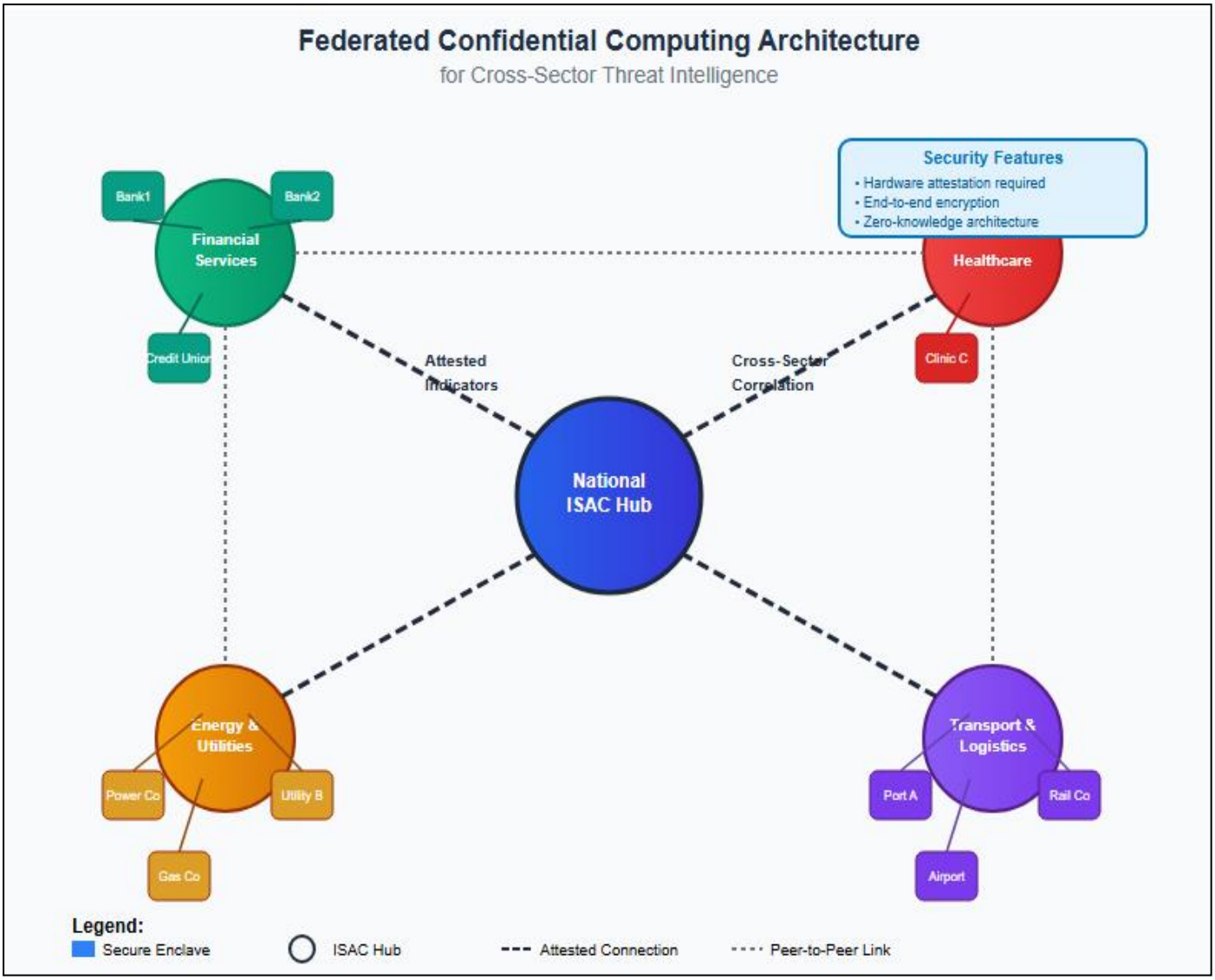

Fig 1 Federated Confidential Computing Architecture

The federated approach addresses several critical challenges in traditional threat intelligence sharing. First, it eliminates the need for centralized data repositories that create attractive targets for adversaries. Second, it enables organizations to maintain direct control over their contributed data while participating in collective analysis. Third, it provides natural scalability as new participants can join the federation without requiring architectural changes to existing deployments.

Network topology design is crucial for maintaining both security and performance in federated enclave deployments. The proposed architecture utilizes a hybrid mesh/star topology where sector-specific Information Sharing and Analysis Centers (ISACs) serve as regional coordination points while maintaining direct peer-to-peer connections between organizations with established trust relationships.

➢ *STIX/TAXII Integration with Confidential Computing*

The integration of confidential computing with established threat intelligence sharing protocols requires careful consideration of data flow architectures and security boundaries. STIX (Structured Threat Information eXpression) provides the semantic framework for representing threat intelligence, while TAXII (Trusted Automated eXchange of Intelligence Information) defines the transport and sharing mechanisms (Dulaunoy et al., 2021).

In the proposed architecture, STIX objects are processed within secure enclaves to extract indicators while preserving the confidentiality of source information. This approach enables organizations to share threat indicators derived from proprietary detection systems without exposing the underlying detection logic or network architecture details that could be exploited by adversaries.

The framework implements a multi-stage processing pipeline where raw STIX objects are ingested into secure enclaves, processed through privacy-preserving analytics to extract relevant indicators, and then formatted for distribution through TAXII channels. This pipeline ensures that only attested, privacy-safe indicators are shared while maintaining the rich semantic structure that makes STIX effective for automated threat response.

Table 3 STIX Object Processing in Secure Enclaves

STIX Object Type	Processing Location	Privacy Transformation	Output Format	Attestation Requirements
Indicator	Secure Enclave	Hash/Pattern Extraction	Anonymized Pattern	Full Platform + Software
Malware	Secure Enclave	Behavioral Analysis	Signature Hashes	Platform + ML Model
Attack Pattern	Standard Processing	Technique Mapping	MITRE ATT&CK TTPs	Standard TLS
Vulnerability	Secure Enclave	Impact Assessment	CVE + Risk Score	Platform Attestation
Threat Actor	Secure Enclave	Attribution Analysis	Campaign Indicators	Full Attestation Required

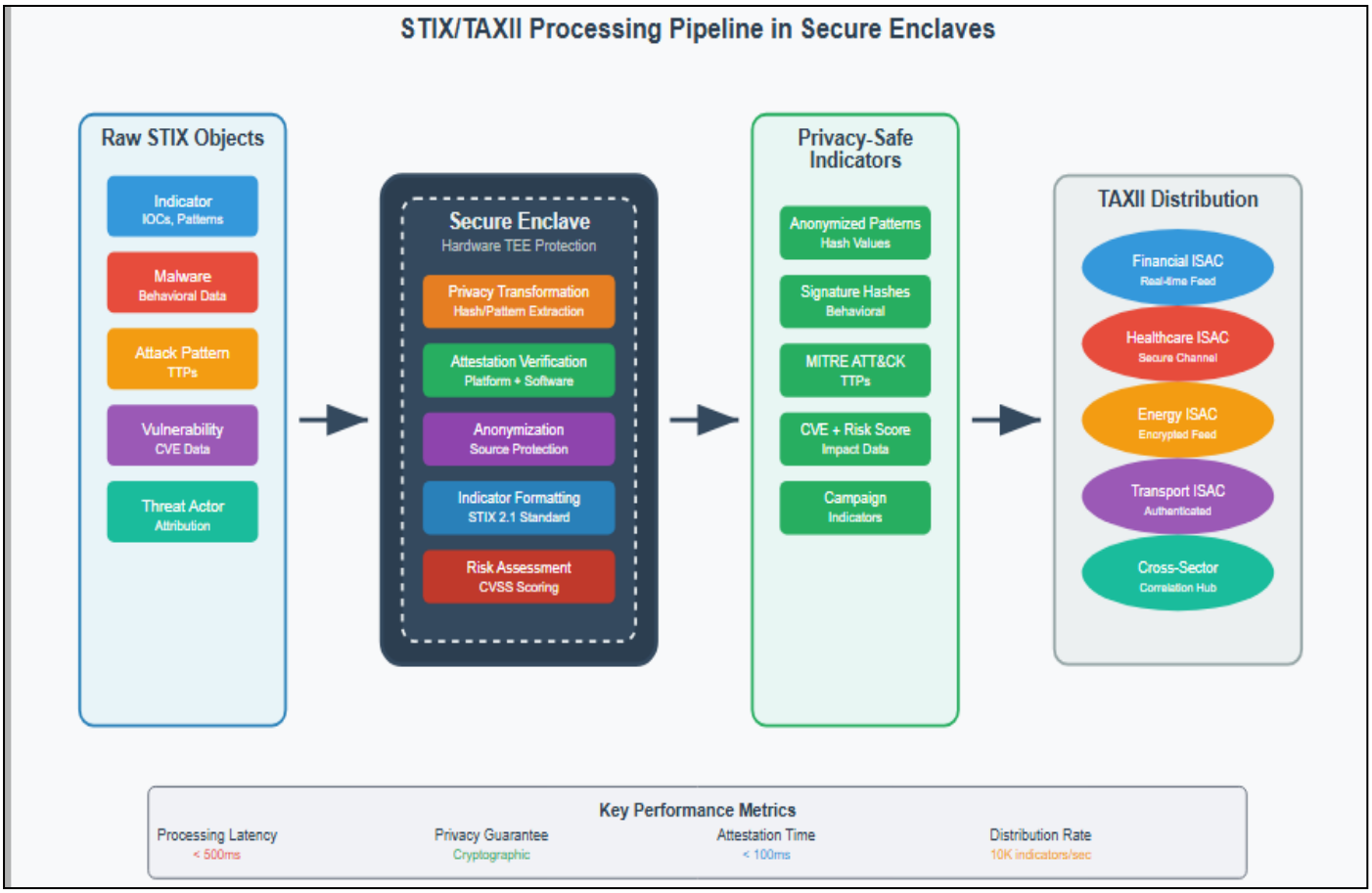

Figure 2 STIX/TAXII Processing Pipeline in Secure Enclaves

➢ *Real-Time Processing and Alert Correlation*

The effectiveness of confidential computing threat exchange depends critically on the ability to process and correlate threat indicators in real-time. Traditional batch processing approaches are insufficient for detecting coordinated attacks that unfold over minutes rather than hours. The proposed architecture implements streaming analytics within secure enclaves to enable sub-minute correlation of threat indicators across sectors.

Real-time processing presents unique challenges in confidential computing environments due to the cryptographic overhead associated with secure enclaves and the limited memory capacity of current implementations. The framework addresses these challenges through optimized streaming algorithms that maintain sliding windows of threat indicators while minimizing memory footprint and computational overhead.

Alert correlation across sectors requires sophisticated algorithms that can identify relationships between disparate threat indicators while operating within the constrained environment of secure enclaves. Machine learning models trained on historical attack patterns enable rapid identification of coordinated campaign indicators, even when individual organizations might miss the broader attack context.

➢ *Cross-Sector Indicator Fusion and Analytics*

The fusion of threat indicators across critical infrastructure sectors presents both opportunities and challenges for collective defense. Different sectors generate distinct types of threat telemetry based on their operational technologies, network architectures, and threat models. Financial institutions, for example, generate high-volume transaction-based indicators, while industrial control systems produce operational technology-specific indicators related to physical processes.

The confidential computing framework enables sophisticated fusion algorithms that can operate across these diverse indicator types while preserving sector-specific privacy requirements. Homomorphic encryption techniques allow for certain types of aggregate analysis without exposing individual sector contributions, while secure multi-party computation enables joint analysis scenarios where multiple sectors must collaborate on sensitive intelligence.

Advanced analytics within secure enclaves can identify subtle patterns that might indicate early stages of coordinated attacks. For example, reconnaissance activities detected by financial institutions might be correlated with infrastructure probing detected by utilities to identify potential campaigns targeting interdependent systems.

V. SECTOR-SPECIFIC IMPLEMENTATION FRAMEWORKS

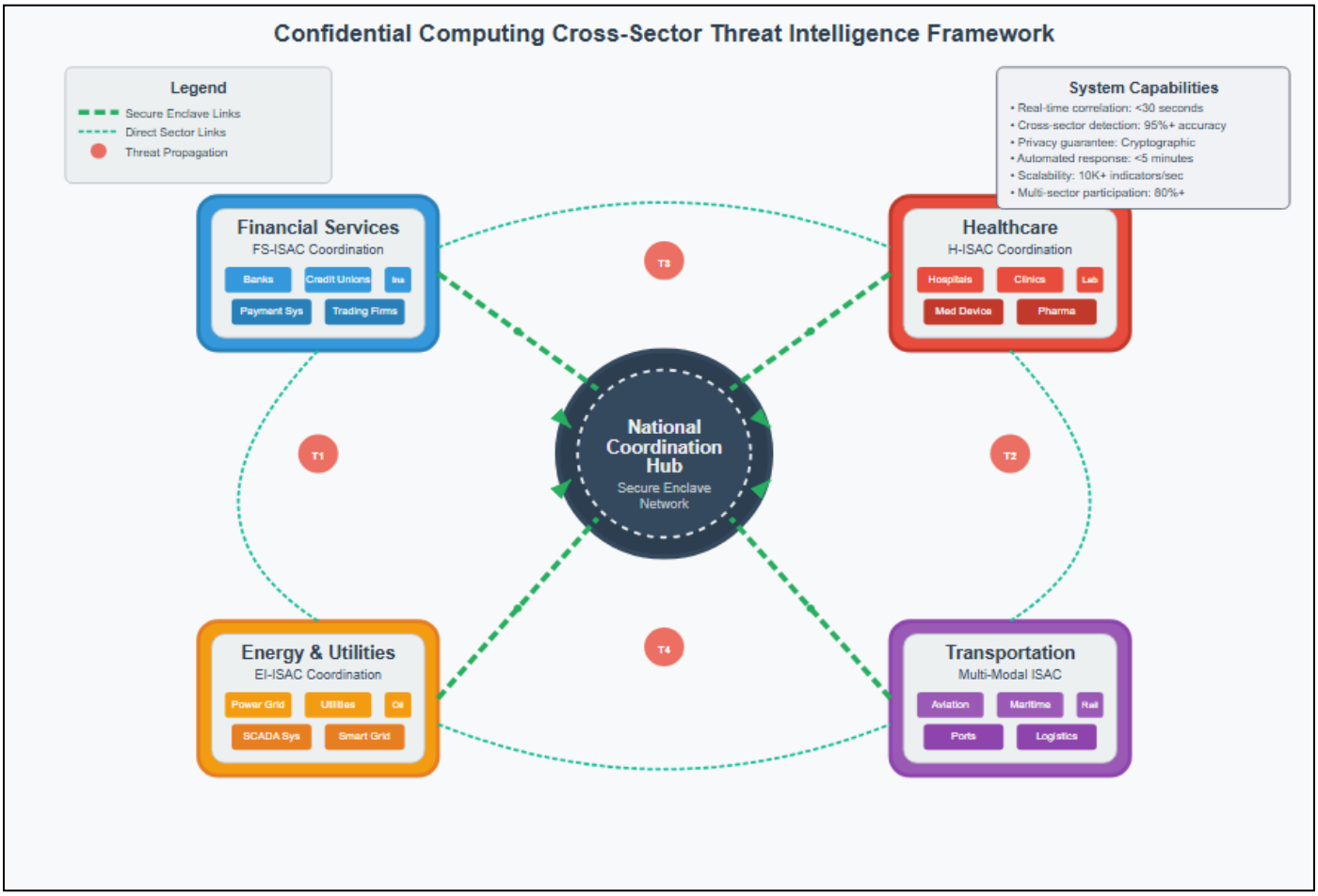

Fig 3 Cross-Sector Implementation Framework

➢ *Financial Services Sector Implementation*

The financial services sector faces unique challenges in threat intelligence sharing due to strict regulatory requirements, competitive concerns, and the high-value nature of the data and systems they protect. The confidential computing approach addresses these challenges by enabling banks and financial institutions to share threat indicators while maintaining compliance with regulations such as the Gramm-Leach-Bliley Act, PCI DSS, and international banking regulations.

Financial institutions generate large volumes of transaction-based threat indicators that can be valuable for detecting fraud, money laundering, and cyber-attacks targeting payment systems. Traditional sharing mechanisms often fail to capture the richness of this data due to privacy concerns and regulatory constraints. Confidential computing enables the processing of transaction patterns within secure enclaves to identify indicators of compromise without exposing sensitive customer or transaction data.

The implementation framework for financial services includes specialized secure enclaves configured for different types of financial threat intelligence. Payment card fraud detection enclaves process transaction patterns to identify indicators of compromised payment systems or fraud networks. Banking malware analysis enclaves examine code samples and behavioral patterns to identify new strains of banking trojans or other financial malware. Market manipulation detection enclaves analyze trading patterns to identify potential cyber-attacks on market infrastructure.

- *Key implementation considerations for the financial sector include:*

✓ *Regulatory Compliance*:
Enclaves must be configured to maintain compliance with banking regulations while enabling effective threat sharing.

✓ *High-Frequency Processing*:
Financial systems generate high-volume, high-frequency data streams that require optimized processing algorithms.

✓ *Cross-Border Considerations:*
International financial institutions must navigate varying regulatory frameworks across jurisdictions.

✓ *Competitive Sensitivity*:
Threat indicators must be processed to remove competitive advantage information while preserving security utility.

➢ *Healthcare Sector Integration*
The healthcare sector presents unique challenges for threat intelligence sharing due to HIPAA privacy requirements, the critical nature of medical systems, and the diverse technology landscape spanning from legacy medical devices to modern electronic health record systems. Confidential computing provides a pathway for healthcare organizations to share threat intelligence while maintaining strict patient privacy protections.

Healthcare organizations are increasingly targeted by ransomware attacks, supply chain compromises, and data theft operations. The sector's threat intelligence sharing has been limited by concerns about exposing protected health information (PHI) and medical system vulnerabilities. Secure enclaves enable healthcare organizations to process threat indicators derived from medical device logs, network traffic analysis, and security event data without exposing patient information or critical system details.

The healthcare implementation framework addresses sector-specific requirements including medical device security, clinical network protection, and research data security. Medical device threat intelligence enclaves process indicators related to vulnerabilities and attacks targeting medical equipment. Clinical network enclaves analyze network traffic patterns to identify threats to electronic health record systems and other clinical applications. Research security enclaves protect intellectual property while enabling collaboration on threats targeting pharmaceutical research and development.

Healthcare-specific considerations for confidential computing implementation include compliance with HIPAA's Technical Safeguards requirements, which mandate specific controls for electronic protected health information (ePHI). Secure enclaves provide a technical means of demonstrating compliance with these requirements while enabling previously impossible forms of threat intelligence collaboration.

The sector faces unique challenges in balancing security requirements with operational continuity. Medical devices often cannot be patched or updated without extensive validation procedures, creating persistent vulnerabilities that require coordinated monitoring across healthcare networks. Confidential computing enables real-time sharing of device vulnerability information without exposing specific hospital configurations or patient care protocols.

Integration with existing healthcare information systems requires careful consideration of interoperability standards such as HL7 FHIR and DICOM. The framework includes specialized adapters that can extract security-relevant information from healthcare data formats while maintaining strict separation between clinical data and threat intelligence processing.

➢ *Energy and Utilities Sector Framework*
The energy and utilities sector represents critical infrastructure that is increasingly targeted by nation-state actors and sophisticated cybercriminal organizations. The sector's unique operational technology (OT) environment, which combines traditional industrial control systems with modern information technology, creates distinct challenges for threat intelligence sharing.

Confidential computing enables utilities to share threat intelligence related to industrial control systems without exposing sensitive information about power generation capacity, grid topology, or operational procedures. This capability is particularly valuable for detecting coordinated attacks that might target multiple utilities simultaneously or attempt to cascade failures across interconnected infrastructure.

The energy sector implementation framework includes specialized enclaves for different types of operational technology threats. SCADA system security enclaves process indicators related to supervisory control and data acquisition systems that monitor and control power generation and distribution. Smart grid security enclaves analyze threats to advanced metering infrastructure and distribution automation systems. Nuclear security enclaves handle the most sensitive threat intelligence related to nuclear power facilities, operating under the strictest security and regulatory requirements.

Power system operators face unique challenges in balancing cybersecurity requirements with operational reliability. The real-time nature of power system operations means that threat response must be integrated with operational procedures to avoid inadvertent impacts on grid stability. Confidential computing enclaves enable rapid sharing of threat indicators while maintaining the operational security necessary for reliable power delivery.

- *Key implementation considerations for the energy sector include:*

✓ *Operational Technology Integration*:
Enclaves must interface with legacy SCADA and distributed control systems while maintaining air-gap security requirements.

✓ *Real-Time Constraints:*
Power system operations require sub-second response times that must be preserved even with additional security processing.

✓ *Regulatory Compliance*:
NERC CIP standards mandate specific cybersecurity controls that must be maintained within confidential computing environments.

✓ *Grid Interdependencies:*
Threat intelligence must account for cascading effects across interconnected transmission and distribution systems.

➢ *Transportation and Logistics Integration*
The transportation sector encompasses diverse subsectors including aviation, maritime, rail, and highway systems, each with distinct operational characteristics and threat models. Modern transportation systems increasingly rely on interconnected networks that span multiple organizational and jurisdictional boundaries, creating opportunities for both enhanced security coordination and potential attack propagation.

Aviation cybersecurity presents particularly complex challenges due to the safety-critical nature of aircraft systems and the international scope of air transportation. Confidential computing enables airlines and airport operators to share threat intelligence related to air traffic control systems, baggage handling networks, and passenger processing systems without exposing operational details that could be exploited by adversaries.

Maritime and port security involves coordination between port operators, shipping companies, and government agencies. Container shipping generates large volumes of logistical data that can reveal patterns relevant to both cybersecurity and physical security. Secure enclaves enable analysis of shipping patterns to identify potential security threats while protecting commercially sensitive cargo information.

Rail transportation systems face unique cybersecurity challenges due to their reliance on legacy signaling systems and the potential for cascading impacts across interconnected networks. Positive Train Control (PTC) systems, which use wireless communications and GPS technology to enhance safety, create new attack surfaces that require coordinated monitoring and threat intelligence sharing.

➢ *Transportation Sector Implementation Priorities Include:*

- *Multi-Modal Coordination*:
Integration across aviation, maritime, rail, and highway systems to detect cross-modal attack campaigns.

- *International Standards:*
Alignment with international transportation security frameworks and cross-border information sharing agreements.

- *Safety Integration*:
Ensuring that cybersecurity measures enhance rather than compromise transportation safety systems.

- *Supply Chain Security:*
Protecting against threats that propagate through transportation and logistics networks.

VI. DETECTION ENGINEERING AND AUTOMATED RESPONSE

➢ *Sandboxed Model Development and Testing*
The effectiveness of confidential computing threat exchange depends critically on the quality and responsiveness of detection algorithms operating within secure enclaves. Traditional approaches to detection engineering often rely on access to large datasets and iterative testing procedures that may conflict with the privacy-preserving goals of confidential computing.

The proposed framework implements sandboxed development environments that enable security researchers to develop and test detection algorithms using synthetic data or carefully anonymized threat intelligence. These sandbox environments utilize the same confidential computing technologies as production deployments, ensuring that detection logic developed in sandbox environments can be deployed seamlessly to production enclaves.

Machine learning model development presents particular challenges in confidential computing environments due to the computational overhead of secure enclaves and the limited visibility into model performance. The framework addresses these challenges through federated learning approaches that enable collaborative model training across multiple organizations without exposing individual datasets.

Table 4 Detection Engineering Workflow in Confidential Computing Environments

Development Stage	Environment	Data Sources	Security Controls	Performance Metrics
Algorithm Design	Local Sandbox	Synthetic Data	Developer Access	Accuracy on Simulated Data
Initial Testing	Isolated Enclave	Anonymized Historical	Code Review + Attestation	False Positive Rate
Cross-Validation	Federated Test Network	Multi-Organization Sample	Remote Attestation	Cross-Sector Performance
Production Deployment	Live Enclave Network	Real-Time Indicators	Full Security Stack	Detection Latency
Continuous Learning	Production + Feedback	Live + Labeled Samples	Automated Updates	Adaptive Performance

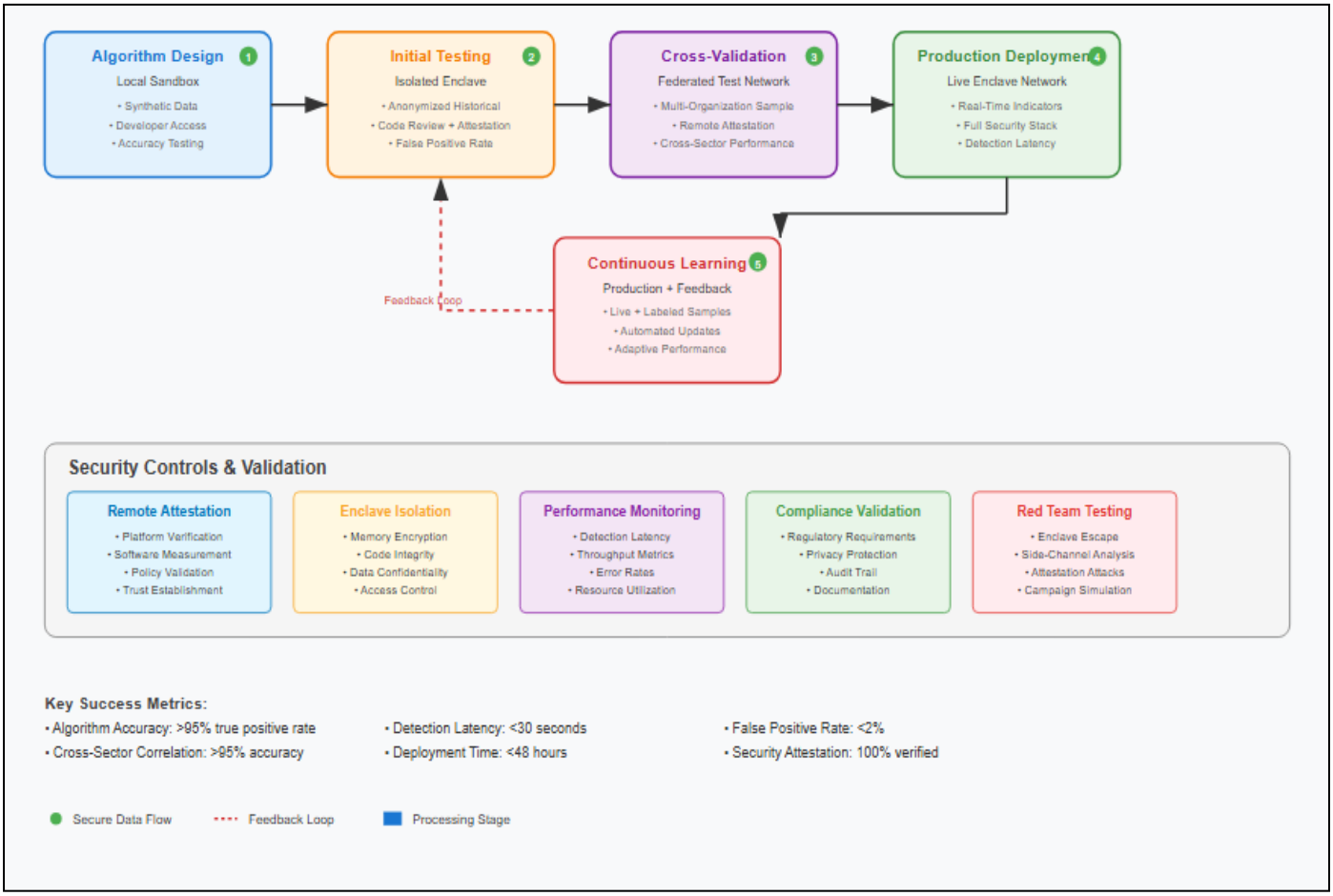

Fig 4 Detection Engineering Workflow

The sandboxing approach enables rapid iteration and testing of detection algorithms while maintaining strict security boundaries. Synthetic data generation techniques create realistic threat scenarios that can be used for algorithm development without exposing sensitive operational information. Privacy-preserving validation techniques enable assessment of algorithm performance across multiple organizations without sharing actual threat data.

➢ *Red Team Integration and Adversarial Testing*

Effective detection engineering requires continuous testing against sophisticated adversarial techniques. Traditional red team exercises often provide limited value for confidential computing environments due to the difficulty of simulating the operational constraints and attack vectors specific to secure enclaves.

The framework incorporates specialized red team capabilities designed specifically for confidential computing threat exchange scenarios. These capabilities include simulation of attacks targeting the attestation infrastructure, attempts to extract sensitive information from secure enclaves through side-channel analysis, and coordination of multi-sector attack campaigns designed to test cross-sector correlation algorithms.

Red team feedback loops are integrated directly into the detection engineering workflow, enabling rapid iteration and improvement of detection algorithms based on observed attack techniques. This integration ensures that detection capabilities evolve continuously to address emerging threats and adversarial techniques.

Adversarial machine learning techniques are particularly relevant for confidential computing environments where attackers may attempt to poison shared threat intelligence or manipulate detection algorithms through carefully crafted inputs. The framework implements robust defenses against adversarial attacks while maintaining the performance characteristics necessary for real-time threat detection.

➢ *Key red team focus areas include:*

- *Enclave Escape Techniques:*
  Testing for vulnerabilities that could allow attackers to break out of secure enclaves.

- *Side-Channel Analysis*:
  Evaluating potential information leakage through timing, power, or electromagnetic side channels.

- *Attestation Attacks:*
  Attempting to forge or manipulate remote attestation procedures.

- *Cross-Sector Campaign Simulation:*
  Coordinated attacks designed to test multi-organization detection and response capabilities

➢ *Automated Response and Orchestration*

The primary value of confidential computing threat exchange lies in enabling rapid, coordinated responses to detected threats. Traditional incident response procedures often rely on manual coordination and communication processes that introduce significant delays and potential points of failure.

The proposed framework implements automated response orchestration that operates within the constraints of confidential computing environments while maintaining human oversight for critical decisions. Response automation focuses on defensive actions that can be taken immediately upon threat detection, such as updating firewall rules, quarantining suspicious network segments, or triggering additional monitoring.

Cross-sector response coordination presents unique challenges due to the diversity of operational environments and regulatory requirements across different critical infrastructure sectors. The framework addresses these challenges through configurable response templates that can be customized for each sector while maintaining interoperability for multi-sector threats.

➢ *Response orchestration includes several key components:*

- *Threat Severity Assessment:*
  Automated evaluation of threat indicators using standardized risk scoring frameworks (CVSS, DREAD) adapted for cross-sector scenarios.

- *Impact Analysis:*
  Assessment of potential cascading effects across interconnected infrastructure systems.

- *Response Template Selection*:
  Automated selection of appropriate response procedures based on threat characteristics and sector-specific requirements.

- *Coordination Protocols:*
  Standardized communication and coordination procedures for multi-organization responses.

➢ *Performance Metrics and Continuous Improvement*

Measuring the effectiveness of confidential computing threat exchange requires sophisticated metrics that account for both security outcomes and operational constraints. Traditional cybersecurity metrics such as detection rates and response times must be augmented with confidential computing-specific measures including attestation latency, enclave performance overhead, and cross-sector correlation accuracy.

Key performance indicators for the framework include detection latency (time from indicator availability to threat identification), correlation accuracy (percentage of correctly identified multi-sector threats), false positive rates (particularly important given the potential for automated responses), and response coordination effectiveness (successful implementation of coordinated defensive actions across sectors).

The framework implements continuous monitoring and improvement processes that operate within confidential computing constraints while enabling system-wide optimization. Federated learning techniques enable improvement of detection algorithms based on collective experience without exposing individual organization data or attack details.

Table 5 Key Performance Metrics for Confidential Computing Threat Exchange

Metric Category	Specific Measures	Target Performance	Measurement Method	Improvement Mechanism
Detection Performance	Time to Detection	< 30 seconds	Automated Logging	Algorithm Optimization
	Cross-Sector Correlation Accuracy	> 95%	Validated Test Cases	Machine Learning Tuning
	False Positive Rate	< 2%	Human Review Feedback	Threshold Adjustment

System Performance	Enclave Processing Latency	< 500ms	Real-time Monitoring	Hardware Optimization
	Attestation Overhead	< 100ms	Network Measurement	Protocol Streamlining
	Throughput Capacity	10K indicators/sec	Load Testing	Scalability Improvements
Operational Effectiveness	Response Coordination Time	< 5 minutes	Workflow Tracking	Process Automation
	Policy Compliance Rate	100%	Audit Verification	Automated Compliance
	Inter-sector Participation	> 80% organizations	Survey Assessment	Incentive Programs

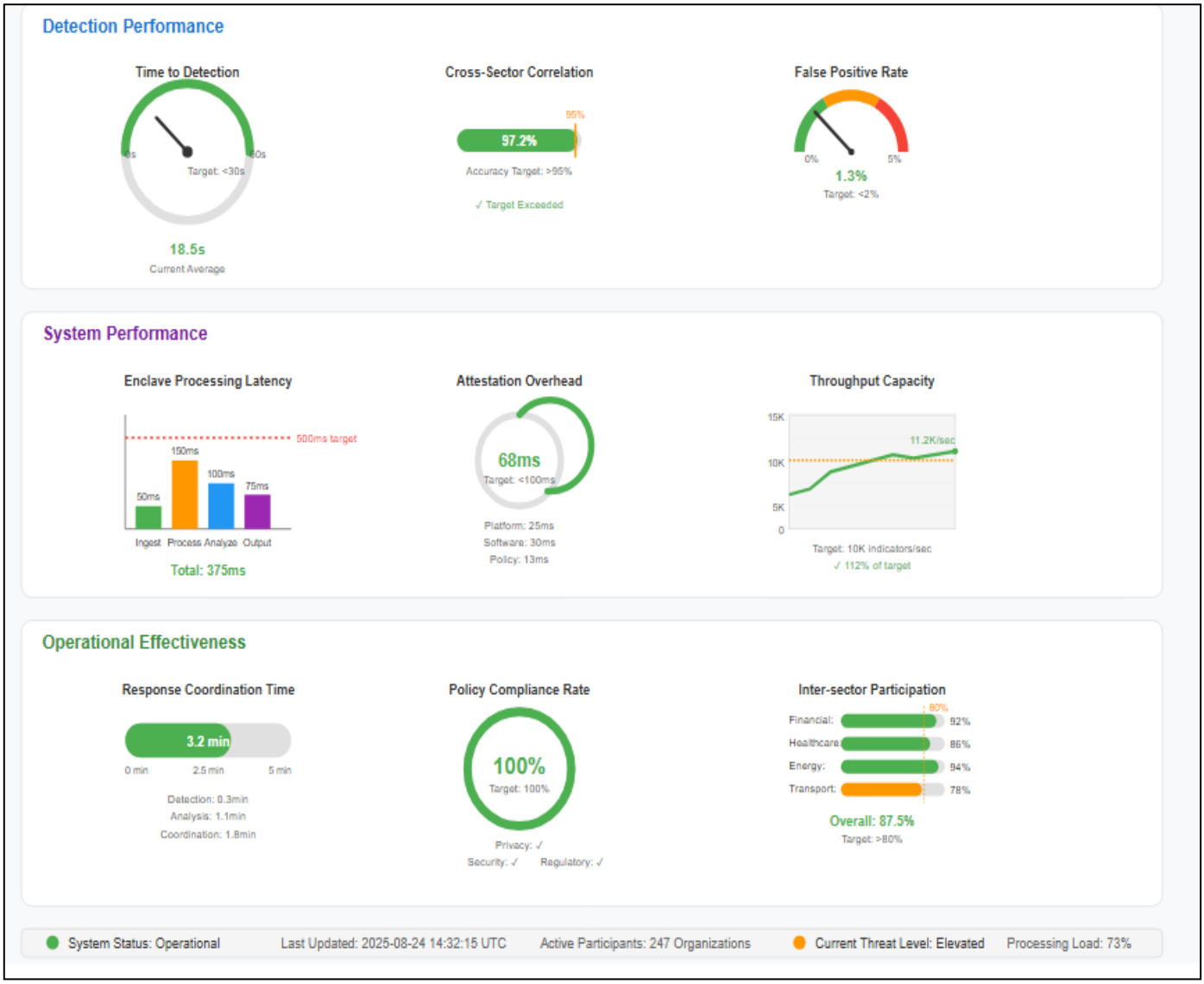

Fig 5 Performance Metrics Dashboard

VII. EVALUATION AND VALIDATION FRAMEWORK

➢ *Simulation Environment and Testing Scenarios*

Validating the effectiveness of confidential computing threat exchange requires sophisticated simulation environments that can accurately model the complex interactions between sectors, threat actors, and detection systems. Traditional cybersecurity testing approaches often fail to capture the full complexity of cross-sector attack campaigns and the operational constraints of critical infrastructure environments.

The evaluation framework utilizes a hybrid simulation approach that combines high-fidelity network emulation with synthetic threat generation to create realistic testing scenarios. This approach enables controlled evaluation of system performance under various threat conditions while maintaining the security

constraints necessary for confidential computing environments.

Testing scenarios are developed based on analysis of historical attack campaigns, threat intelligence reports, and red team exercises specifically designed for critical infrastructure environments. These scenarios include coordinated attacks across multiple sectors, supply chain compromises that propagate through interconnected systems, and sophisticated persistent threats that operate over extended time periods.

Table 6 Validation Testing Scenarios and Metrics

Scenario Category	Test Scope	Key Metrics	Expected Performance	Validation Method
Single-Sector Attack	Individual ISAC	Detection Latency	< 30 seconds	Network Emulation
Cross-Sector Campaign	Multiple ISACs	Correlation Accuracy	> 95% true positive	Synthetic Data Injection
Supply Chain Compromise	Interconnected Organizations	Propagation Detection	< 60 seconds cross-sector	Historical Replay
Advanced Persistent Threat	Long-term Multi-Vector	Pattern Recognition	> 90% campaign detection	Red Team Exercise
Resource Exhaustion	High-Volume Attack	System Resilience	< 5% performance degradation	Load Testing

The simulation environment includes accurate models of sector-specific network architectures, realistic traffic patterns, and authentic threat intelligence data streams. Advanced threat modeling techniques simulate sophisticated adversaries with knowledge of confidential computing systems and cross-sector interdependencies.

➢ *Privacy and Security Validation*

Confidential computing threat exchange requires rigorous validation of privacy and security guarantees to ensure that sensitive information is protected throughout the sharing and analysis process. Traditional security testing approaches must be augmented with specific techniques for validating confidential computing implementations.

Security validation includes comprehensive testing of attestation mechanisms, evaluation of side-channel resistance, and validation of cryptographic implementations. Privacy validation focuses on ensuring that shared threat intelligence cannot be used to infer sensitive information about participating organizations or their operational environments.

The framework implements formal verification techniques for critical security properties, including information flow analysis to ensure that sensitive data cannot leak from secure enclaves and cryptographic protocol verification to validate the correctness of key management and attestation procedures.

➢ *Privacy validation techniques include:*

- *Differential Privacy Analysis*:

Verification that shared threat indicators provide mathematically guaranteed privacy protections.

- *Information Leakage Testing*:

Systematic evaluation of potential data leakage through various channels.

- *Adversarial Analysis:*

Testing against sophisticated attackers attempting to extract sensitive information.

- *Compliance Verification*:

Validation that privacy protections meet sector-specific regulatory requirements.

➢ *Operational Readiness Assessment*

Successful deployment of confidential computing threat exchange requires careful assessment of organizational readiness and operational compatibility. This assessment encompasses technical infrastructure requirements, organizational processes and procedures, and regulatory compliance considerations.

Technical readiness assessment includes evaluation of computing infrastructure capable of supporting confidential computing workloads, network connectivity and bandwidth requirements for real-time threat intelligence sharing, and integration capabilities with existing security operations centers and incident response procedures.

Organizational readiness encompasses staff training and development requirements, incident response procedure updates to accommodate automated response capabilities, and legal and regulatory compliance verification for cross-sector information sharing.

Table 7 Organizational Readiness Assessment Framework

Assessment Domain	Readiness Criteria	Measurement Approach	Minimum Requirements
Technical Infrastructure	CC Hardware, Network Capacity	Capability Assessment	SGX/SEV/CCA Support

Personnel Training	Security Operations Skills	Competency Evaluation	80% Staff Certified
Process Integration	SOC Procedure Updates	Workflow Analysis	< 10% Process Changes
Regulatory Compliance	Legal Framework Alignment	Compliance Audit	100%Requirement Coverage
Inter-organizational Trust	Sharing Agreement Execution	Partnership Assessment	Bilateral Agreements

VIII. REGULATORY AND POLICY CONSIDERATIONS

➢ *Legal Framework Requirements*

The implementation of confidential computing threat exchange across critical infrastructure sectors must navigate complex legal and regulatory frameworks that vary by sector, jurisdiction, and type of information shared. Current regulatory approaches often lag behind technological capabilities, creating uncertainty about the legal status of automated threat intelligence sharing and cross-sector coordination.

Key legal considerations include data protection and privacy regulations such as GDPR, CCPA, and sector-specific privacy requirements, cybersecurity regulatory frameworks including NIST Cybersecurity Framework and sector-specific standards, cross-border information sharing restrictions and export control regulations, and liability frameworks for automated defensive actions that might impact other organizations or systems.

The confidential computing approach provides significant advantages for regulatory compliance by enabling organizations to demonstrate that sensitive information is protected through cryptographic means rather than procedural controls alone. This capability may enable new forms of information sharing that would be prohibited under traditional approaches due to privacy or competitive concerns.

- *Legal Framework Considerations Include:*

✓ *Privacy Regulation Compliance:*

Ensuring that threat intelligence sharing mechanisms comply with applicable privacy laws while enabling effective security collaboration.

✓ *Liability Management:*

Establishing clear frameworks for responsibility and liability in automated response scenarios.

✓ *Cross-Border Data Flows:*

Addressing legal restrictions on international information sharing while maintaining global threat intelligence capabilities.

✓ *Regulatory Harmonization:*

Working toward consistent regulatory approaches across sectors and jurisdictions.

➢ *International Cooperation and Standards*

Critical infrastructure protection increasingly requires international cooperation due to the global nature of both critical infrastructure systems and the threat landscape. Confidential computing threat exchange must be designed to operate across international boundaries while respecting varying national security and privacy requirements.

International standards development is crucial for ensuring interoperability and maintaining security guarantees across different implementations and jurisdictions. The framework contributes to emerging standards in confidential computing, threat intelligence sharing, and critical infrastructure protection.

- *Key International Cooperation Considerations Include:*

✓ *Standards Harmonization*:

Development of international standards for confidential computing-enabled threat intelligence sharing.

✓ *Mutual Recognition*:

Establishment of frameworks for recognizing confidential computing attestation procedures across national boundaries.

✓ *Data Sovereignty:*

Respecting national requirements for data localization while enabling effective threat intelligence sharing.

✓ *Treaty and Agreement Frameworks:*

Integration with existing international cybersecurity cooperation agreements and development of new frameworks as needed.

Policy recommendations include development of international frameworks for confidential computing-enabled threat intelligence sharing, harmonization of critical infrastructure protection requirements across allied nations, and establishment of mutual recognition frameworks for confidential computing attestation procedures.

IX. FUTURE RESEARCH DIRECTIONS

➢ *Advanced Confidential Computing Technologies*

The continued evolution of confidential computing technologies presents opportunities for enhanced threat intelligence sharing capabilities. Emerging technologies such as fully homomorphic encryption, secure multi-party computation, and advanced trusted execution environments may enable new forms of privacy-

preserving analysis that are not feasible with current approaches.

Quantum-resistant cryptography development is particularly important for long-term deployment of confidential computing threat exchange systems. The framework must be designed to accommodate future cryptographic upgrades without requiring fundamental architectural changes. Post-quantum cryptographic algorithms will need to be integrated into all components of the system, from attestation procedures to data encryption protocols.

Integration with emerging computing paradigms such as edge computing and distributed systems architectures may enable new deployment models that bring threat intelligence processing closer to the sources of threat data while maintaining security and privacy guarantees.

- *Advanced confidential computing research areas include:*

✓ *Homomorphic Encryption Integration:*
Enabling computation on encrypted threat intelligence data without decryption.

✓ *Secure Multi-Party Computation:*
Facilitating collaborative analysis across multiple organizations without revealing individual inputs.

✓ *Verifiable Computing:*
Ensuring that threat intelligence processing produces provably correct results.

✓ *Quantum-Safe Protocols:*
Developing threat intelligence sharing mechanisms that remain secure against quantum computing attacks.

➢ *Artificial Intelligence and Machine Learning Integration*

The integration of advanced artificial intelligence and machine learning capabilities with confidential computing presents both opportunities and challenges for threat intelligence sharing. Privacy-preserving machine learning techniques may enable more sophisticated threat detection and analysis while maintaining the confidentiality requirements of critical infrastructure organizations.

Federated learning approaches show particular promise for enabling collaborative development of threat detection models without exposing individual organization data. However, significant research is needed to address challenges including model poisoning attacks, differential privacy guarantees, and computational efficiency within secure enclaves.

Automated reasoning and decision support systems may enhance the effectiveness of human oversight in confidential computing threat exchange systems. These systems must be designed to operate within the constraints of secure enclaves while providing the transparency and explain ability necessary for critical infrastructure applications.

- *AI and ML Research Priorities Include:*

✓ *Privacy-Preserving ML:*
Developing machine learning algorithms that can operate on encrypted or anonymized threat intelligence data.

✓ *Federated Learning Optimization:*
Improving the efficiency and security of collaborative model training across multiple organizations.

✓ *Adversarial ML Defense:*
Protecting machine learning models from poisoning and evasion attacks in threat intelligence scenarios.

✓ *Explainable AI:*
Ensuring that AI-driven threat detection and response systems provide clear reasoning for their decisions

➢ *Scalability and Performance Optimization*

As confidential computing threat exchange systems grow to encompass larger numbers of participants and higher volumes of threat intelligence data, scalability and performance optimization become critical research challenges. Current confidential computing technologies introduce computational overhead that may limit the scalability of real-time threat intelligence processing.

Research into optimized algorithms and architectures specifically designed for confidential computing environments is needed to achieve the performance characteristics required for national-scale threat intelligence sharing. This includes development of efficient cryptographic protocols, optimized data structures for secure enclaves, and parallel processing techniques that can operate within confidential computing constraints.

- *Scalability Research Priorities Include*:

✓ *Performance Optimization*:
Developing algorithms and data structures specifically optimized for confidential computing environments.

✓ *Distributed Processing:*
Creating frameworks for distributing threat intelligence processing across multiple secure enclaves.

✓ *Network Optimization:*
Improving the efficiency of threat intelligence distribution and synchronization across large-scale deployments.

✓ *Resource Management:*

Developing intelligent resource allocation and load balancing techniques for confidential computing workloads.

X. CONCLUSION

This research presents a comprehensive framework for confidential computing-enabled threat intelligence exchange that addresses the critical need for enhanced collaboration in cybersecurity while preserving the privacy and operational security requirements of critical infrastructure organizations. The proposed approach leverages hardware-based trusted execution environments, standardized threat intelligence protocols, and automated response mechanisms to create a national early-warning system capable of detecting and mitigating coordinated attacks across sectors.

The key contributions of this work include a detailed architectural framework that integrates confidential computing with established threat intelligence sharing protocols, sector-specific implementation guidelines that address the unique requirements of financial services, healthcare, energy, and transportation sectors, and a comprehensive evaluation methodology that validates both security and operational effectiveness of the proposed approach.

The analysis demonstrates that confidential computing threat exchange can significantly reduce the time required to detect and respond to cross-sector attacks, from hours or days to minutes, while maintaining strict privacy protections for participating organizations. The framework enables sharing of attested threat indicators without exposing sensitive operational data, addressing a fundamental barrier to effective threat intelligence collaboration.

The framework's impact on national cybersecurity resilience is substantial. By enabling real-time sharing of threat indicators across critical infrastructure sectors, the system creates a collective defense capability that is greater than the sum of its individual components. The automated response mechanisms ensure that defensive actions can be coordinated across sectors within minutes of threat detection, dramatically reducing the window of opportunity for successful attacks.

Implementation challenges include the need for specialized hardware infrastructure, development of standardized protocols for cross-sector interaction, and establishment of legal and regulatory frameworks that support automated threat intelligence sharing. However, the potential benefits for national cybersecurity resilience justify the required investments in technology and policy development.

The economic benefits of the framework extend beyond direct cybersecurity improvements. By reducing the impact of successful cyberattacks and enabling more efficient use of cybersecurity resources across sectors, the system provides substantial return on investment. The privacy-preserving nature of the approach also enables new forms of collaboration that would be impossible under traditional information sharing frameworks.

Future research directions include integration of advanced artificial intelligence and machine learning capabilities, development of quantum-resistant cryptographic protocols, and expansion to international threat intelligence sharing networks. The continued evolution of confidential computing technologies promises to enable even more sophisticated forms of privacy-preserving collaboration that can adapt to emerging threats and operational requirements.

The framework presented in this paper provides a foundation for transforming how critical infrastructure organizations collaborate on cybersecurity, moving from ad-hoc information sharing to automated, real-time collective defense capabilities. By preserving privacy while enabling effective collaboration, confidential computing threat exchange represents a paradigm shift toward more resilient and responsive critical infrastructure protection.

REFERENCES

[1]. Adeshina, Y. T. (2021). Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. *International Journal of Engineering Technology Research & Management*, 5(12), 204-218.

[2]. Adeshina, Y. T., & Ndukwe, M. O. (2024). Establishing a blockchain-enabled multi-industry supply-chain analytics exchange for real-time resilience and financial insights. *IRE Journals*, 7(12), 599-610. https://doi.org/10.5281/zenodo.16053081

[3]. Adeshina, Y. T., Owolabi, B. O., & Olasupo, S. O. (2023). A U.S. national framework for quantum-enhanced federated analytics in population health early-warning systems. *International Journal of Engineering Technology Research & Management*, 7(2), 76-95. https://doi.org/10.5281/zenodo.15589483

[4]. Ali, A., & Awad, A. I. (2018). Cyber threat intelligence: A literature review. *Journal of Information Security and Applications*, 41, 1–16. https://doi.org/10.1016/j.jisa.2018.05.007

[5]. Alhajjar, E., Maxwell, P., & Bastian, N. (2021). Adversarial machine learning in network intrusion detection systems. *Expert Systems with Applications*, 168, 114241. https://doi.org/10.1016/j.eswa.2020.114241

[6]. Asghari, H., van Eeten, M., & Bauer, J. M. (2015). Cybersecurity information sharing: Measuring benefits and risks. *Journal of Cybersecurity*, 1(1), 19–35. https://doi.org/10.1093/cybsec/tyv005

[7]. Barnum, S. (2020). Interoperability challenges in cyber threat intelligence sharing using

STIX/TAXII. *Computers*, 9(1), 18. https://doi.org/10.3390/computers9010018

[8]. Bamigbade, O., Adeshina, Y. T., & Kasali, K. (2024). Ethical and explainable AI in data science for transparent decision-making across critical business operations. *International Journal of Engineering Technology Research & Management*, 8(11), 734-753. https://doi.org/10.5281/zenodo.15671481

[9]. Carrapico, H., & Farrand, B. (2016). Trust and information sharing: Information Sharing and Analysis Centers (ISACs) and U.S. policy. *Journal of Cyber Policy*, 1(2), 235–254. https://doi.org/10.1080/23738871.2016.1229804

[10]. Carter, D., Bittleston-Khan, S., & Wright, I. (2024). Current approaches and future directions for cyber threat intelligence sharing. *Journal of Information Security and Applications*, 78, 103690. https://doi.org/10.1016/j.jisa.2024.103690

[11]. Delignat-Lavaud, A., Pironti, A., Standaert, F.-X., & Warinschi, B. (2023). Why should I trust your code? *Communications of the ACM*, 66(12), 24–26. https://doi.org/10.1145/3624578

[12]. Dhanuskodi, J., Pursley, M., Proctor, A., & Shah, G. (2023). Creating the first confidential GPUs. *Communications of the ACM*, 66(12), 38–41. https://doi.org/10.1145/3626827

[13]. Dulaunoy, A., Wagener, G., & Iklody, A. (2021). The MISP threat sharing platform: Experiences and lessons learned. *Digital Threats: Research and Practice*, 2(3), 1–19.

[14]. Han, J., Xing, X., & Chen, K. (2023). Confidential computing and related technologies: A critical review. *Cybersecurity*, 6, 28. https://doi.org/10.1186/s42400-023-00144-1

[15]. Harrison, S., Pritchard, O., & Popov, P. (2022). Overcoming information-sharing challenges in cyber defence. *Journal of Cybersecurity*, 8(1), tyac001. https://doi.org/10.1093/cybsec/tyac001

[16]. Kaplan, D. (2023). Hardware VM isolation in the cloud. *Communications of the ACM*, 66(12), 30–32. https://doi.org/10.1145/3624576

[17]. Khatoun, R., & Khoukhi, L. (2022). Confidential computing in cloud/fog-based IoT scenarios: A review. *Array*, 13, 100134. https://doi.org/10.1016/j.array.2022.100134

[18]. Komarov, M., Bernšteins, A., & Levchenko, O. (2022). Secure and efficient exchange of threat information using TAXII and private blockchain. *Information*, 13(10), 463. https://doi.org/10.3390/info13100463

[19]. Kwon, D., Kim, H., & Lee, S. (2021). Cybersecurity training for critical infrastructure protection: A systematic review. *International Journal of Critical Infrastructure Protection*, 33, 100441. https://doi.org/10.1016/j.ijcip.2021.100441

[20]. Lazouski, A., Ferraiolo, D. F., & Mont, M. C. (2021). Privacy-preserving data sharing infrastructures for healthcare: A review. *BMC Medical Informatics and Decision Making*, 21, 288. https://doi.org/10.1186/s12911-021-01602-x

[21]. Li, Z., Wang, Y., Liu, J., & Zhu, H. (2024). Survey of research on confidential computing. *IET Communications*, 18(5), 627–646. https://doi.org/10.1049/cmu2.12759

[22]. McMillan, R., Pithadia, S., & Stein, M. (2024). Threat hunting: Evolving techniques and detection engineering practices. *Journal of Network and Computer Applications*, 236, 104939. https://doi.org/10.1016/j.jnca.2024.104939

[23]. Russinovich, M. (2024). Confidential computing: Elevating cloud security and privacy. *Communications of the ACM*, 67(1), 26–28. https://doi.org/10.1145/3624577

[24]. Rüsch, D., & Vigna, G. (2020). On the design of collaborative cyber-defense systems with trusted execution. *IEEE Access*, 8, 151040–151059.

[25]. Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

[26]. Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved? A survey on the dimensions of cyber threat intelligence sharing. *Computers & Security*, 60, 154–176. https://doi.org/10.1016/j.cose.2016.04.014

[27]. Sun, W., Qian, H., & Zhang, X. (2021). Efficient and privacy-preserving malware detection based on Intel SGX. *Future Generation Computer Systems*, 117, 230–242.

[28]. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence: Steps, challenges and issues. *Computers & Security*, 72, 212–234. https://doi.org/10.1016/j.cose.2017.09.001

[29]. Yoon, C., Lee, J., & Kim, T. (2022). A comprehensive study of AMD SEV-SNP and Intel TDX for confidential VMs. *ACM Queue*, 20(6), 20–39. https://doi.org/10.1145/3700418

[30]. Yusuff, T. A. (2025). A neuro-symbolic artificial intelligence and zero-knowledge blockchain framework for a patient-owned digital-twin marketplace in U.S. value-based care. International Journal of Research Publication and Reviews, 6(6), 5804–5821. https://doi.org/10.55248/gengpi.6.0625.21105

[31]. Yusuff, T. A. (2023a). Interoperable IT architectures enabling business analytics for predictive modeling in decentralized healthcare ecosystem. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 346–355. https://doi.org/10.14569/IJACSA.2023.0141144

[32]. Yusuff, T. A. (2023b). Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 359–370. https://doi.org/10.14569/IJACSA.2023.0141146

[33]. Yusuff, T. A. (2023c). Multi-tier business analytics platforms for population health surveillance using federated healthcare IT infrastructures. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 338–345. https://doi.org/10.14569/IJACSA.2023.0141143

[34]. Yusuff, T. A. (2023d). Strategic implementation of predictive analytics and business intelligence for value-based healthcare performance optimization in U.S. health sector. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 327–337. https://doi.org/10.14569/IJACSA.2023.0141142