Cyber security in ICT Demand Distribution: Provocations and Frame work

D. Poovizhi[a], M. Kema[b], N. Mariya Jennifer[b], K. Arulmozhi[b], R. Sakthi Sri[b]

a Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur- 613006, Tamil Nadu, India

b Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur- 613006, Tamil Nadu, India

Abstract-In an increasingly interconnected world, the integrity and security of Information and Communication Technology (ICT) supply chains are paramount. As organizations rely more on technology to conduct business and store sensitive data, the risks associated with cyber threats within the ICT supply chain escalate. This abstract delves into the demands of cyber security within the ICT supply chain and the essential strategies to mitigate associated risks. Compliance with regulatory frameworks and industry standards is essential for mitigating cyber security risks within the ICT supply chain. Adhering to standards such as ISO 27001, NIST Cybersecurity Framework, and GDPR facilitates the implementation of best practices and ensures a baseline level of security across the supply chain ecosystem.

Keywords— ICT; Cyber Security; SIEM; Blockchain;

I. INTRODUCTION

In recent years, understanding the intricate nature of the ICT supply chain is imperative. It encompasses a network of vendors, manufacturers, distributors, and service providers, each presenting potential vulnerabilities. Threat actors exploit these vulnerabilities through various means, including malware injection, supply chain attacks, and insider threats. Recognizing and addressing these risks require a holistic approach to cyber security.

Establishing robust security protocols throughout the supply chain lifecycle is crucial. This involves implementing stringent vetting procedures for suppliers, ensuring the integrity of hardware and software components, and monitoring for suspicious activities continuously. Additionally, fostering transparency and collaboration among supply chain stakeholders can enhance threat intelligence sharing and incident response capabilities.

II. LITERATURE SURVEY

In practice, an efficient resilience strategy would ideally leverage the following three main components: (i) continuous availability, enabled by both the deployment of strategies to guarantee an "always-on" customer experience, and the required protection in front of disruptions; (ii) IT workload mobility, permitted by the deployment of strategies facilitating traffic offloading and resource migration in a distributed computing environment, includ ing edge and cloud computing; and (iii) multi-cloud agility (also including hybrid clouds and coordinated edge-cloud), to determine the optimal set of resources that best match the expected level of resilience for each application. These three components are driving the deployment of the corresponding policies to provide security, trust, and performance guar antees, coupled with efficient network and compute infrastructure management strategies, in order to optimize the resource allocation, self-healing, and dynamic reconfiguration of ICT resources.

Cybersecurity is one of the greatest challenges of our era. In May 2017, the WannaCry malware cyber attack infected more than 200,000 computers across 150 countries, with the total damages estimated to be hundreds of millions of Euros [3]. During the same year, more than 26% of US healthcare consumers experienced a breach of their healthcare data, which included their social security number, contact information, electronic medical record, or health insurance ID [4]. This is hugely reflected and significantly amplified in the supply chain realm, among several other factors, because of the potential of the so-called domino effect. According to [5], there were reports of a worm "Stuxnet" that reportedly infiltrated Siemens industrial control software and later impacted the operation of an Iranian nuclear plant through the ICT supply chain. Also, in [6], it was reported that

components of the Boing airliner were failing due to glitches in the Japanese supply chain production that globally affected airports and grounded airliners in India, Chile, and the United States. In [7], the authors reported, from their work in an EU project, that the major crimes encountered by supply chain stakeholders in Europe were theft in transit (23%), data theft/cybercrime (11%), bogus companies (10%), and insider fraud (10%). Also, other crimes were reported, including smuggling (9%), counterfeiting (9%), and terrorism (6%). Less frequent in the past, but possibly a bigger threat in the future, were also environmental crimes in the supply chain [8].

III. CHALLENGES

Challenge 1- Need for end-to-end solutions for vulnerabilities and risks management:

End-to-end solutions are scalable and flexible, capable of adapting to the evolving needs and requirements of organizations of all sizes and industries. Whether managing a small number of vulnerabilities or addressing complex security challenges at enterprise scale, these solutions provide the scalability and flexibility needed to accommodate diverse environments and use cases.

Challenge 2- Lack of evidence-based metrics for security assurance and trust guarantees:

Evidence-based metrics are essential for providing objective insights into security assurance and trust guarantees, enabling organizations to quantify their security posture, demonstrate assurance to stakeholders, benchmark performance, inform decision making, drive continuous improvement, and enhance resilience to cyber threats. Addressing the lack of such metrics requires collaboration among industry stakeholders, standardization efforts, and investments in research and development to develop robust and actionable metrics for cybersecurity.

Challenge 3- Cumbersome coordination in multi-actor and multi-vendor supply chains of ICT systems:

ICT systems in multi-vendor supply chains may suffer from interoperability issues due to differences in technology standards, protocols, and interfaces. Integrating disparate systems and components from multiple vendors requires careful coordination and testing to ensure compatibility and functionality. Multi-actor and multi-vendor supply chains introduce security and compliance risks, including data breaches, intellectual property theft, and regulatory violations. Coordinating security measures, risk assessments, and compliance efforts across the supply chain is essential to mitigate these risks effectively.

Challenge 4- Static cybersecurity networked configurations and dynamic systems audit:

Even when a security policy is successfully developed and implemented, the security systems in use are rather static with respect to the highly dynamic threat prevention and mitigation techniques needed. In most of the cases, neither the network elements nor the security appliances support a reconfiguration framework to meet the pace of the highly dynamically changing nature of cyber threats. The ease of attacking an ICT supply chain is largely due to the network. In fact, the network actually significantly amplifies the security threat in the supply chain.

IV. EXISTING SYSTEM

The existing FISHY architecture aims at delivering a coordinated cyber-resilient platform that would provide the appropriate set of tools and methods towards establishing trusted supply chains of ICT systems, through novel evidence-based security assurance methodologies and metrics, as well as innovative strategies for risk estimation and vulnerabilities forecasting leveraging state-of-the-art solutions, leading to resilient complex ICT systems, comprising the complete supply chain, particularly focusing on the IoT devices at the edge and the network systems connecting them. Addressing the challenges 1 to 4, the proposed architecture is not envisioned as an incremental integrated cybersecurity solution, but rather as an extensible and programmable framework that can flexibly orchestrate the whole set of ICT systems and security controls. The aim is to provide an innovative cyber resilience framework, where complex ICT systems performance in an entire supply chain may be analyzed, in terms of the security, trust, and privacy impact on performance. To this end, the proposed architecture seamlessly combines advancements in several domains, including software-defined networking (SDN), network function virtualization (NFV), intent-based networking, AI-based techniques, and distributed ledger technologies (DLT). The main concept relies on designing a security, trustworthy, and certification layer, transversal to the whole set of stakeholders in the supply chain, intended to make the entire ICT supply chain system resilient, but also to correctly measure the complete security

compliance and consequently trigger the required actions (mitigation, reconfiguration, etc.).

Problems in Existing System

i. Insecure communication channels, unverified suppliers, or compromised components.

ii. Data breaches, malware infections, or supply chain disruptions, leading to financial losses and reputational damage.

iii. Counterfeit or Substandard Components.

iv. Lack of Transparency and Accountability.

V. Proposed System

Temporal–Spatial hybrid market trend forecasting model (TSMTF) which integrates the information of ICT supply chain network bidding, enterprise sector attribute and time sequence. In addition, can better improve the prediction effect, and the method can be directly applied in practice.

Temporal Dimension:

Time-based Analysis: Considerations of time include factors such as data access timestamps, event sequencing, time intervals between events, and historical trends. This dimension enables the analysis of data over time to identify patterns, trends, and anomalies, supporting tasks such as predictive analytics, trend forecasting, and anomaly detection.

Temporal Context: Understanding the temporal context of ICT systems involves recognizing how events and activities evolve over time, such as user interactions, system performance fluctuations, and service availability changes. Temporal context enables the dynamic adaptation of ICT systems to changing conditions and requirements, supporting tasks such as dynamic resource allocation and workload optimization.

Spatial Dimension:

Location-based Considerations: Spatial considerations involve factors such as geographical location, physical proximity, network topology, and distribution of resources. This dimension enables the analysis of data and activities in relation to their spatial context, supporting tasks such as geospatial analysis, location-based services, and network optimization.

Spatial Context: Understanding the spatial context of ICT systems involves recognizing how physical locations and spatial relationships impact system behavior and performance, such as network latency, bandwidth availability, and resource proximity. Spatial context enables the optimization of ICT systems for distributed environments, supporting tasks such as edge computing, content delivery, and network caching.

Hybrid Model Integration:

Temporal-Spatial Correlation: The hybrid model integrates temporal and spatial dimensions to capture the correlations between time-based and location-based factors. This integration enables the analysis of spatiotemporal patterns, relationships, and dependencies within ICT systems, supporting tasks such as context-aware computing, situational awareness, and real-time decision making.

Dynamic Adaptation: The hybrid model facilitates the dynamic adaptation of ICT systems based on both temporal and spatial factors, allowing for context-aware optimization, resource allocation, and workload management. This adaptability enhances system resilience, efficiency, and responsiveness to changing environmental conditions and user requirements.

Potential Benefits:

Enhanced Insights: The temporal-spatial hybrid model provides deeper insights into the behavior and performance of ICT systems by considering both time and space dimensions.

Dynamic Optimization: The hybrid model supports dynamic optimization of ICT systems based on real-time data and contextual information, enhancing system agility, efficiency, and effectiveness.

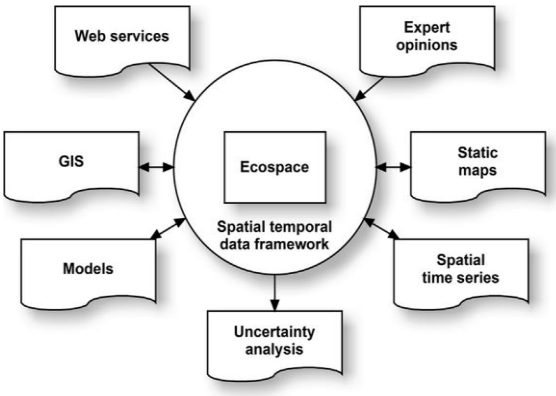

Fig 1. Temporal Spatial Analysis

VI WORKING

Geospatial Data Collection: Spatial analysis begins with the collection of geospatial data, which includes information tied to specific geographic locations or coordinates. This data can be collected from various sources, such as GPS devices, satellite imagery, geographic information systems (GIS), and location-based services (LBS).

Data Integration and Processing: Geospatial data is integrated with other relevant data sets, such as demographic data, environmental data, infrastructure data, or business data. This integrated data is processed and prepared for analysis, including data cleaning, normalization, and transformation to ensure consistency and accuracy.

Spatial Visualization: Spatial analysis often involves visualizing geospatial data on maps or spatial representations. Geographic information systems (GIS) and mapping tools are used to create maps, charts, and visualizations that depict spatial patterns, relationships, and distributions within the data.

Spatial Query and Analysis: Spatial analysis techniques are applied to explore spatial patterns, relationships, and trends within the data. Common spatial analysis methods include:

Spatial Queries: Queries that retrieve data based on spatial relationships, such as proximity, containment, or intersection with specific geographic features.

Spatial Join: Combining data from different layers or data sets based on their spatial relationships, such as overlaying demographic data on a map of census tracts.

Spatial Interpolation: Estimating values at unsampled locations based on nearby sampled data points, such as predicting pollution levels across a region based on air quality sensor data.

Spatial Regression: Statistical modeling techniques that account for spatial autocorrelation, spatial heterogeneity, and other spatial dependencies in the data.

Hot Spot Analysis: Identifying clusters or concentrations of high or low values within the data, such as crime hot spots or disease outbreaks.

Network Analysis: Analyzing spatial networks, such as transportation networks or utility networks, to optimize routing, logistics, and resource allocation.

Decision Making and Planning: The insights gained from spatial analysis inform decision making and planning processes in various domains, including urban planning, environmental management, public health, transportation, disaster response, and business operations. Spatial analysis helps identify opportunities, mitigate risks, and optimize resource allocation based on geographic considerations.

VII CONCLUSION

In conclusion, spatial analysis offers valuable insights into the complexities of the ICT (Information and Communication Technology) supply chain by examining data and phenomena within the context of geographic locations or spatial relationships. Through the integration of geospatial data with other relevant datasets and the application of spatial analysis techniques, organizations can better understand and manage various aspects of the ICT supply chain.

Overall, spatial analysis of the ICT supply chain enables organizations to unlock new opportunities, mitigate risks, and optimize operations by leveraging geographic context and spatial relationships. By integrating spatial analysis into their supply chain management practices, organizations can achieve greater visibility, efficiency, and resilience in the dynamic and interconnected world of ICT supply chain operations.

VIII FUTURE ENHANCEMENT

Future enhancements will involve the use of spatial simulation and optimization techniques to model and optimize supply chain networks. Simulation models will enable organizations to test various scenarios, evaluate the impact of changes, and identify optimal configurations for their ICT supply chain operations. Integration of blockchain technology with spatial analysis will facilitate secure and transparent tracking of goods and transactions across the ICT supply chain. Blockchain-based spatial tracking solutions will provide immutable records of supply chain events, enhance traceability, and ensure data integrity and authenticity. Augmented reality (AR) technologies will enable immersive spatial visualization of supply chain data, allowing stakeholders to interact with geospatial information in 3D environments. AR-based spatial visualization tools will enhance situational awareness, decision-making, and collaboration among supply chain partners.

VIII REFERENCES

[1] Ross, R.; Graubart, R.; Bodeau, D.; McQuaid, R. Systems Security Engineering: Cyberresiliency Considerations for the Engineering of
Trustworthy Secure Systems; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018; Volume 2.
[2] Orrey, K. Cyber Attack: Exploiting the User—There Are So Many Ways! MSc Computer Security and Forensics. Ph.D. Thesis,
University of Bedfordshire, Luton, UK, 2010.
[3] From the Puget Sound Business Journal. 3:00 am PST, Boeing 787 Battery Lags behind Evolving Lithium-Ion Technology. Available
online: http://www.bizjournals.com/seattle/print-edition/2013/02/15/lithium-ion-battery-technology-has.html (accessed
on 15 February 2013).
[4] Urciuoli, L.; Männistö, T.; Hintsa, J.; Khan, T. Supply Chain Cyber Security—Potential Threats. Inf. Secur. Int. J. 2013, 29,
51–68. [CrossRef]
[5] Development of a Strategic Roadmap towards a Large Scale Demonstration Project in European Logistics and Supply Chain
Security, LOGSEC Deliverable. 31 March 2011. (accessed on 16 April 2021).
[6] Symantec, The Cyber Resilience Blueprint: A New Perspective on Security, While Paper. (accessed on 16 April 2021).
[7] Hamlen, K.W. Stealthy Software: Next-generation Cyber-attacks and Defenses. In Proceedings of the 2013 IEEE International
Conference on Intelligence and Security Informatics, Seattle, WA, USA, 4–7 June 2013.
[8] Masip-Bruin, X.; Ren, G.; Serral-Gracia, R.; Yannuzzi, M. Unlocking the Value of Open Data with a Process-based Information
Platform. In Proceedings of the 2013 IEEE 15th Conference on Business Informatics, Vienna, Austria, 15–18 July 2013.
[9] Research Reveals Organizations. Falling behind in Cybersecurity Analytics and Operations Despite Business Pressure to Improve,
Businesswire. 2017.
[10] Kahvazadeh, S.; Barbosa, V.; Masip-Bruin, X.; Marín-Tordera, E.; Garcia, J.; Diaz, R. Securing combined Fog-to-Cloud System
through SDN approach. In Proceedings of the 4th Workshop on CrossCloud Infrastructures & Platforms, Belgrade, Serbia,
23–27 April 2017.