International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Securing Supply Chain Networks

Chris Gilbert[1], Mercy Abiola Gilbert[2], Maxwell Dorgbefu Jnr[3], Duah Jeremiah Leakpor[4], Kwitee D. Gaylah[5], Isaac A. Adetunde[6]
[1456]Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman University
[2]Department of Guidance and Counseling/College of Education/William V.S. Tubman University/
[3]Department of Information Technology Education/Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED), Ghana
Corresponding Author Email Address: cabilimi@tubmanu.edu.lr

Abstract— *This paper investigates the multifaceted security challenges inherent in modern supply chain networks (SCNs), emphasizing the vulnerabilities introduced by the integration of cyber-physical systems (CPS) and ultra-large-scale CPS (ULS-CPS). Amid intensified global competition and the growing reliance on outsourcing, SCNs have become both strategic assets and potential targets for sophisticated cyber-physical attacks. By presenting a holistic threat model that spans the entire CPS topology, this study critically examines key vulnerabilities such as third-party risks, the complexity of interconnected systems, and a pervasive lack of transparency in decision-making. A rigorous qualitative analysis, supported by a comparative evaluation of both software integrity verification and hardware security measures, reveals that even minor degradations in network resilience can lead to significant operational and financial losses. Novel metrics for assessing SCN robustness are proposed, alongside cross-disciplinary recommendations that integrate insights from transportation policy, cybersecurity, and supply chain management. The findings underscore the necessity for an integrated, continuous risk management framework to ensure long-term resilience and operational continuity in the face of emerging technological threats.*

Keywords— *Supply Chain Networks, Cyber-Physical Systems, Risk Management, Third-Party Risks, Software Integrity Verification, Hardware Security Measures, Holistic Threat Modeling, Resilience Metrics, Transparency, Cross-Disciplinary Integration.*

I. INTRODUCTION

Effective supply chain networks (SCNs) offer numerous strategic benefits to organizations (Vyas, Dasgupta & Sošic, 2024; Gilbert, 2022). By enabling the analysis of customer demand and the optimization of production logistics, SCNs help identify bottlenecks, balance cost and quality trade-offs, test strategic configurations, and evaluate innovative process improvements (Elahi et al., 2023; Gilbert, Gilbert & Dorgbefu Jnr, 2025b). In an era of intensified global competition and increased reliance on outsourcing, firms are shifting their focus to core competencies while integrating internal production with external suppliers and distributors. Concurrently, innovative technologies are being deployed to optimize operations, reduce delivery times and costs, and shorten time-to-market (Bhamra et al., 2022; Gilbert, 2018).

In today's dynamic business environment, the success of an enterprise critically hinges on its ability to produce and distribute high-quality products both rapidly and cost-effectively (Lim, 2023; Gilbert, 2021). At the heart of this capability lies an effective SCN, which is fundamentally an integrated system comprising organizations, people, activities, and technology (Liebowitz, 2019; Gilbert & Gilbert, 2025c). SCNs can range from simple warehouse management to complex systems that track the flow of materials and services from suppliers through to the end consumer.

1.1. Background and Significance

The increasing integration of cyber-physical systems (CPS) with the physical world introduces significant new risks (Kholidy, 2021; Gilbert et al., 2025). As threats propagate across ultra-large-scale CPS (ULS-CPS), issues such as cross-layer vulnerabilities, insider threats, privacy loss, and collateral damage become more pronounced. This interconnectedness necessitates that different domains address varying levels of trust and implementation policies, requiring continuous monitoring, verification, and certification of trustworthiness. Securing the supply chain is especially critical in this context (Rosado et al., 2022; Gilbert, 2012).

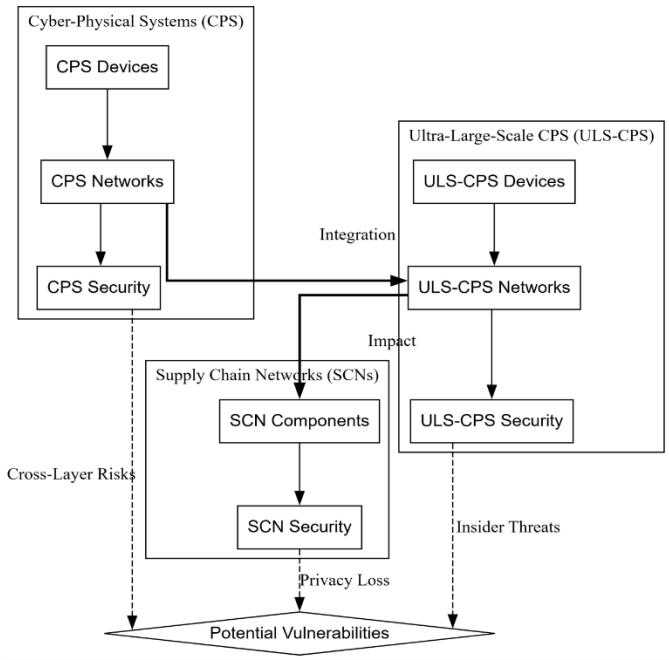

Figure 1: The relationship between different components of Cyber-Physical Systems (CPS) and Ultra-Large-Scale CPS (ULS-CPS).

Over the past decade, growing attention has been directed toward the security of isolated CPS, such as distributed control

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

systems (DCS), supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICS), which are increasingly vulnerable to sophisticated cyber threats (Sheikh et al., 2022; Opoku-Mensah, Abilimi & Amoako, 2013). The emergence of ULS-CPS compounds these challenges, calling for comprehensive and systematic risk assessments that span multiple domains (Kumar, Marston & Sen, 2020; El-Kady et al., 2023; Christopher, 2013). This paper presents a holistic threat model that encompasses the entire CPS topology and underscores the crucial role of supply chain security throughout the development, operation, and maintenance phases.

The diagram outlines the structure of Cyber-Physical Systems (CPS) and Ultra-Large-Scale CPS (ULS-CPS), focusing on how they are connected and their associated risks. CPS and ULS-CPS consist of devices, networks, and security components. These systems interact with supply chain networks (SCNs), which also have their own components and security measures. The diagram highlights cross-layer risks, including integration challenges, the potential impact of vulnerabilities, privacy loss, and insider threats.

1.2 Research Questions

1. How can supply chain networks be secured against emerging cyber-physical threats and evolving technologies?
2. What are the primary vulnerabilities in modern supply chain networks, particularly regarding third-party risks, system complexity, and transparency issues?
3. How effective are current software integrity verification and hardware security measures in mitigating supply chain attacks?
4. What novel metrics can be developed to assess the robustness and resilience of supply chain networks?
5. How can a cross-disciplinary security strategy be formulated to enhance the overall resilience of supply chain networks?

1.3 Research Objectives

Main Research Objective

To develop a comprehensive framework that enhances the security and resilience of supply chain networks by integrating technological innovations, robust risk management practices, and cross-disciplinary strategies.

Specific Research Objectives

i. To investigate and document the current vulnerabilities in supply chain networks, with emphasis on cyber-physical integration and emerging technological risks.
ii. To identify and critically assess key challenges—including third-party risks, network complexity, and lack of transparency—that affect security in modern supply chains.
iii. To evaluate existing measures for software integrity verification and hardware security, and explore potential improvements or novel approaches.
iv. To propose and validate novel metrics to measure the robustness and resilience of supply chain networks.
v. To formulate integrated, cross-disciplinary strategies that encompass transportation policy, supply chain management, and cybersecurity to mitigate risks effectively.

1.4 Methodology

The research approach adopted in the article can be summarized as follows:

i. *Literature Review and Background Research:* A thorough review of existing academic and industry literature was conducted to understand traditional and emerging challenges in securing supply chain networks, as well as to identify gaps in current risk management strategies (shown in *Figure 2*).
ii. *Conceptual and Holistic Threat Modeling:* The authors developed a holistic threat model that encompasses the entire cyber-physical topology of supply chain networks. This model maps out potential vulnerabilities from the integration of CPS to the decentralized nature of modern supply chains (shown in *Figure 3*).
iii. *Qualitative Analysis of Vulnerabilities:* Through a detailed qualitative assessment, the study explored key issues such as third-party risks, the complexity of interconnected systems, and transparency deficits in decision-making processes.
iv. *Evaluation of Security Measures:* The methodology included a comparative analysis of both software-based and hardware-based security measures:
    a. Software Integrity Verification: Focused on current practices like digital signatures, build process controls, and the role of trusted code signers.
    b. Hardware Security Measures: Assessed approaches such as heterogeneous multiprocessor architectures and dynamic instruction set variations to prevent side-channel attacks (shown in *Table 1*).
v. *Development of Novel Metrics:* The research introduced new metrics designed to assess the robustness and resilience of supply chain networks, aiming to quantify the impact of minor degradations and overall network performance.
vi. *Cross-Disciplinary Integration:* Insights from transportation policy, network security, and supply chain management were integrated to form recommendations that extend beyond isolated technical solutions.
vii. *Case Studies and Scenario Analysis:* Practical examples and case studies (e.g., discussions of state-led initiatives and industry-specific challenges) were used to illustrate how vulnerabilities can cascade through complex supply chains and to validate the proposed models and metrics.
viii. *Synthesis and Recommendations:* Finally, the findings were synthesized to draw conclusions about the current state of supply chain security, and strategic recommendations were provided for industry-led initiatives and further research directions (El-Kady et al., 2023; Kumar, Marston & Sen, 2020; Sheikh et al., 2022; Opoku-Mensah, Abilimi & Boateng, 2013).

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

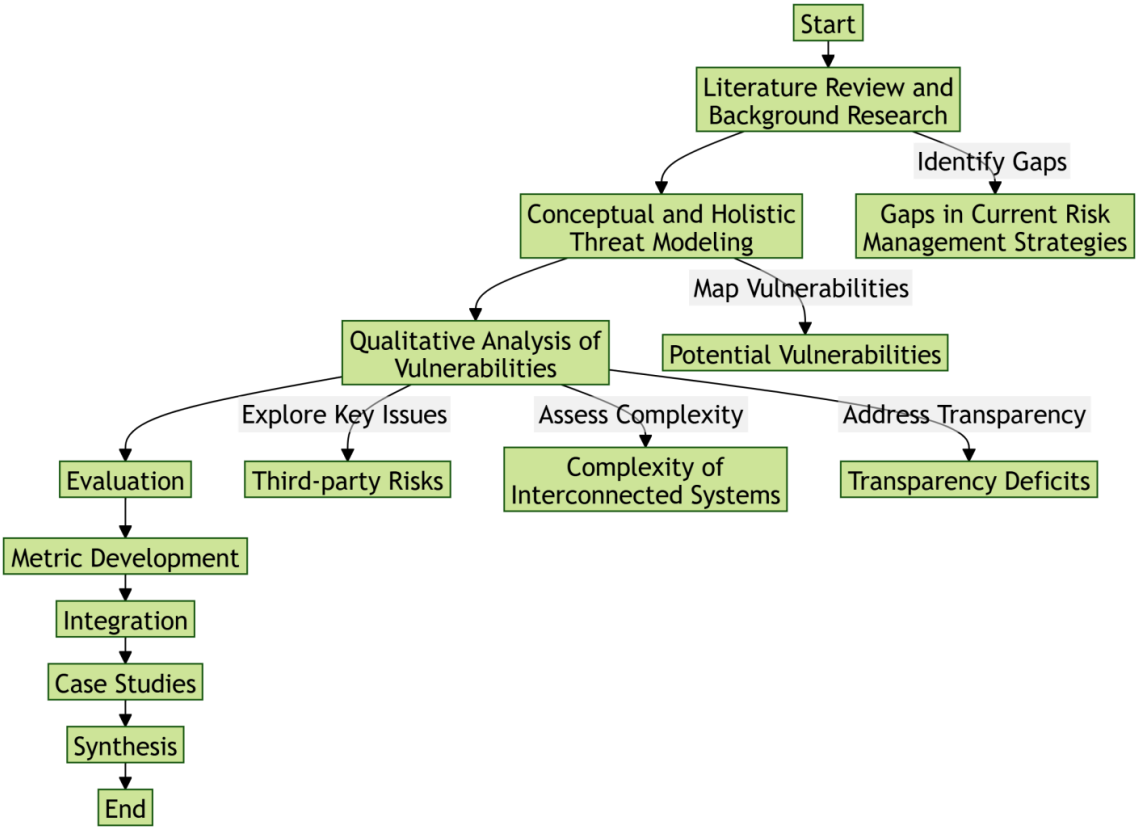

Figure 2: A process flowchart.

TABLE 1: Software Integrity Verification vs. Hardware Security Measures

Security Measure	Strengths	Weaknesses	Application Contexts
Software Integrity Verification			
Digital Signatures	- Ensures authenticity of code and data. - Public key infrastructure makes it highly scalable.	- Computationally expensive, especially with large datasets. - Can be vulnerable to key compromise.	- Code signing in software distribution. - Ensuring software integrity in secure communications.
Build Process Controls	- Ensures the integrity of software development processes. - Can catch unauthorized modifications early.	- Relies on the security of the build environment. - May not detect malicious insiders within the build system.	- Used in secure software development pipelines. - Protecting against supply chain attacks.
Trusted Code Signers	- Provides verification of code origin. - Prevents the installation of unauthorized software.	- Key management challenges. - Dependency on certificate authorities (CA).	- Securing software distribution platforms. - Verifying authenticity in app stores.
Hardware Security Measures			
Heterogeneous Multiprocessor Architectures	- Provides inherent isolation between different processors. - Reduces the risk of cross-processor attacks.	- Increased complexity in system design. - Potential compatibility issues with legacy software.	- High-performance computing environments. - Systems requiring diverse computational tasks (e.g., cloud computing).
Dynamic Instruction Set Variations	- Reduces risks of side-channel attacks. - Dynamic adjustments can increase unpredictability for attackers.	- Increased hardware complexity. - Potential performance overhead.	- High-security applications requiring continuous instruction set protection. - Protection in multi-user systems.

This diagram outlines a structured methodology for evaluating vulnerabilities and assessing risk management strategies, particularly focusing on identifying gaps in current systems and addressing the complexity and transparency issues that emerge from interconnected systems. The flowchart emphasizes the importance of qualitative analysis, third-party risks, and the development of metrics for evaluating these factors.

Each approach has its strengths in particular contexts, with software-based measures more suited for ensuring software integrity in development and distribution, while hardware-based measures are better for high-security environments where protection from advanced persistent threats is critical.

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

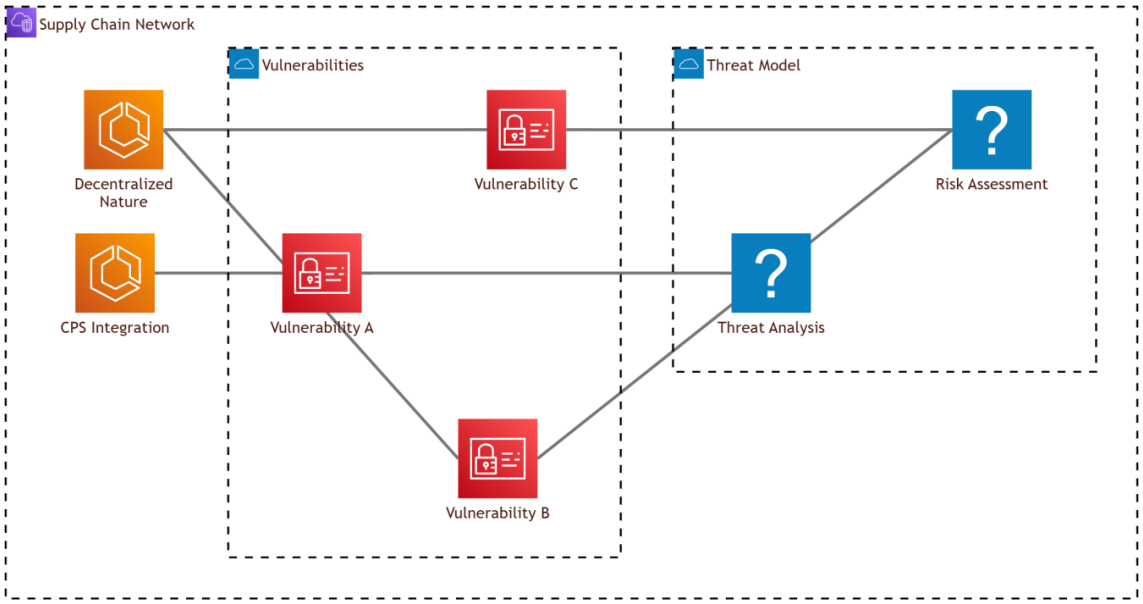

Figure 3: A process for evaluating vulnerabilities and risks within a supply chain network.

The diagram represents a structured approach for assessing risks in a supply chain network by considering its decentralized nature, CPS integration, and the vulnerabilities that could arise from these factors. The flow of the process moves from identifying the vulnerabilities to mapping them into a threat model, analyzing the potential threats, and performing a final risk assessment to evaluate the overall risk level.

II. Challenges in Securing Supply Chain Networks

Securing physical supply chain networks (SCNs) presents significant challenges (Becklines, 2024; Gilbert & Gilbert, 2025d). Traditional methods that rely on centralized physical delivery points for inspecting and verifying suppliers' goods could be rendered obsolete by emerging technologies such as mass 3-D printing and photonic machining, which have the potential to decentralize these processes (Hasan et al., 2022; Gilbert & Gilbert, 2025e). For example, some state governments, like Idaho in the US, have already begun to offer specialized add-on services. These emerging "fifth-party" providers could extend specialized functions, such as food claims audits to the SCN industry, mirroring the evolution seen in the trucking industry where centralized, formal service providers have replaced informal, in-house solutions (Habibi et al., 2025; Gilbert, Gilbert & Dorgbefu Jnr, 2025a).

Figure 4: The various challenges in securing supply chain networks

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

As interfacing technologies become more accessible and large multinational corporations consolidate their business models, small and medium-sized enterprises (SMEs) operating within networked supply chains face exponentially increasing threats and risks (Hasan et al., 2023; Gilbert & Gilbert, 2025f). The entry point for both technological collaboration and cyber-attacks, including the distribution of malware, is shifting towards smaller businesses. In this environment, the implementation of intelligent transportation systems and collaborative networks can enhance operational efficiency and reduce logistics costs while still preserving the security of both goods and data (Yeboah, Opoku-Mensah & Abilimi, 2013a). In a model that emphasizes collaborative regions, key data elements such as arrival notices and digital certificates might be generated or managed by specialized fifth-party service providers, similar to current providers of centralized payroll or administrative services (Zekhnini et al., 2021; Yeboah, Opoku-Mensah & Abilimi, 2013b).

This diagram outlines the various challenges in securing supply chain networks, emphasizing the complexity and interconnectedness of modern systems. Cyberattacks, malware distribution, and third-party risks are significant threats, while emerging technologies introduce new vulnerabilities. The decentralization of processes and the lack of transparency further complicate security efforts. Additionally, data management issues and limited visibility in supply chains make it harder to detect and mitigate risks (Gilbert & Gilbert, 2025h). The effects of these challenges can influence operational effectiveness, the safety of products and information, and might even cause holdups in the movement of goods. Smaller enterprises may also struggle to implement robust security measures, making them more vulnerable.

2.1. Third-Party Risks

A common safeguard against third-party risks is the deployment of Virtual Private Networks (VPNs) for medium-to-large suppliers, supported by policies that require such protection based on the supplier's assigned risk rating (Vaidya, 2019; Gilbert et al., 2025). Sensitive data, particularly that which is classified as top secret or legally binding, is often subject to stringent access controls that permit transmission only between a sponsor and an authorized secondary party (Gilbert & Gilbert, 2024y). These measures may be integrated into the supplier's existing infrastructure, or suppliers may be required to adhere to the sponsor's security conditions.

Typically, a supply chain involves a direct relationship between a sponsor and a supplier engaged in delivering a specific product or service. However, many modern supply chains are considerably more complex and involve multiple entities, including logistics companies that facilitate the movement of goods between suppliers and sponsors (Gilbert, Auodo & Gilbert, 2024; Alsmadi & Easttom, 2020). A primary concern for sponsors is that a supplier's IT security may be less robust than their own, a risk that is exacerbated when suppliers have direct access to sensitive information. Ensuring secure communications and protecting shared resources when accessed remotely by suppliers remains a critical challenge in managing third-party risks (UK, 2020; Abilimi & Yeboah, 2013).

This analysis underscores the necessity for comprehensive risk management strategies that address not only internal security practices but also the broader vulnerabilities inherent in complex, multi-party supply chain networks.

TABLE 2: The Risk Assessment Matrix for third-party risks

Identified Risk	Likelihood (1-5)	Impact (1-5)	Risk Score (Likelihood x Impact)
Third-party IT Security Weaknesses	4	5	20
Insecure Communication	3	4	12
Remote Access to Sensitive Data	5	5	25
Supplier Access to Sensitive Information	4	5	20
Logistics Company Involvement	3	3	9

The table lists identified risks, their likelihood and potential impact, and a calculated risk score (likelihood multiplied by impact). This quantitative summary helps assess and prioritize vulnerabilities in the context of third-party risks within the supply chain.

2.2. Complexity and Interconnectedness

Governments have advocated for structural containment measures over suppliers; however, the specific nature, scale, and extent of such containment need to be reconsidered (Graefrath, 2023; Gilbert, Oluwatosin & Gilbert, 2024). Supply chain networks are inherently complex, with disruptions at lower tiers capable of cascading through the entire system. Notably, large-scale players frequently emerge as common denominators across disrupted supply chains (Shifrinson, 2020; Gilbert & Gilbert, 2024x). Some scholars have proposed models—such as those focusing on dominant "tyrannical" players or employing order parameter approaches—as potential alternatives for managing the intricate interconnections in high-technology industries. Yet, an open question remains: can overly simplified models adequately capture the multifaceted dynamics of modern supply chains?

High-tech nodes and links, which become particularly critical under elevated demand, are high-value targets and essential for maintaining system discipline and establishing robust safeguards (Can, 2024; Gilbert & Gilbert, 2025g). A comprehensive understanding of the technical logistics cycle is crucial, as conventional, simplified drawdown models often fall short in capturing these complexities. While military supply chains sometimes exhibit unique "stay-behind" characteristics, the prevailing paradigm in commercial and high-tech environments is one of dominant, large-scale providers. In such networks, the interconnectedness among multiple suppliers cannot be effectively managed merely by reducing the number or strength of interconnections (Gilbert & Gilbert, 2024v). Although robust primary providers are indispensable, lean supply chains often lack adequate secondary sources, rendering them vulnerable; the disruption of a single component may

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

precipitate broader systemic failures. Indeed, academic research has historically focused more on elucidating the mechanisms behind system failures rather than on the factors that enable system survival (Kim, 2022; Gilbert & Gilbert, 2024w).

2.3. Lack of Transparency

A further challenge in modern supply chain networks is the pervasive lack of transparency in decision-making at key delivery nodes (Vafadarnikjoo et al., 2023; Gilbert & Gilbert, 2024v). These nodes are often occupied by corporate entities that unilaterally set demand levels, schedules, and delivery terms in ways that predominantly serve their own interests or those of select partners (Yeboah, Odabi & Abilimi Odabi, 2016). For instance, in one illustrative case, actors within "Network X" employed a strategy that evolved from cautious to aggressive tactics, manipulating delivery quantities to secure an unfair advantage over the market (Sobb, Turnbull & Moustafa, 2020; Yeboah & Abilimi, 2013). This advantage was maintained through practices such as bypassing conventional money services networks, manipulating industry standards, concealing critical documents, and selectively partnering with preferred players.

The implications of such opacity extend beyond individual transactions (Kumar, Liu & Shan, 2020; Gilbert & Gilbert, 2024u). As noted by Gim and Waller, the absence of transparency not only distorts the operational dynamics of the supply chain network but also undermines the formation of an equitable Pareto frontier, ideally a balanced representation of contributions from all network participants. In many instances, the measures used to establish this frontier are determined without any binding agreements or contracts that guarantee mutual profit or success (Lynberg & Deif, 2023 Gilbert & Gilbert, 2024t). Instead, the level of Pareto dominance reflects an ad hoc balance, where one network may contribute a significant demand while another contributes only minimally (Gilbert & Gilbert, 2024s; Udeh et al., 2024). Consequently, across various combinations of demand levels and delivery rates, the overall system consistently exhibits a lack of transparency, ultimately compromising both efficiency and fairness in real-time operations (Al-Farsi, Rathore & Bakiras, 2021; Gilbert & Gilbert, 2024r).

III. Techniques for Preventing Supply Chain Attacks

This paper examines the established methods attackers employ to compromise the supply chain and provides insights that help organizations and users comprehend the array of potential threats. Although these techniques and their countermeasures are not novel, their recurring nature enables a clearer understanding of attacker objectives and facilitates the prioritization of defensive measures (Tahmasebi, 2024; Gilbert & Gilbert, 2024q). Many of these countermeasures are already incorporated, wholly or partially, into the standard procedures of a Security Operations Center (SOC) (Abdelkader et al., 2024; Gilbert & Gilbert, 2024p). By becoming familiar with these well-documented techniques, supply chain stakeholders can better anticipate their occurrence, whether used individually or in combination, and thereby bolster their resilience against a broad spectrum of compromise strategies (Gilbert & Gilbert, 2024n; Aslaner, 2024). Importantly, the scope of supply chain threats extends beyond overt physical tampering or the insertion of malware during manufacturing; for instance, attackers may deploy malware through non-blueprint-based methods, thus expanding the potential risk landscape (Gilbert & Gilbert, 2024o).

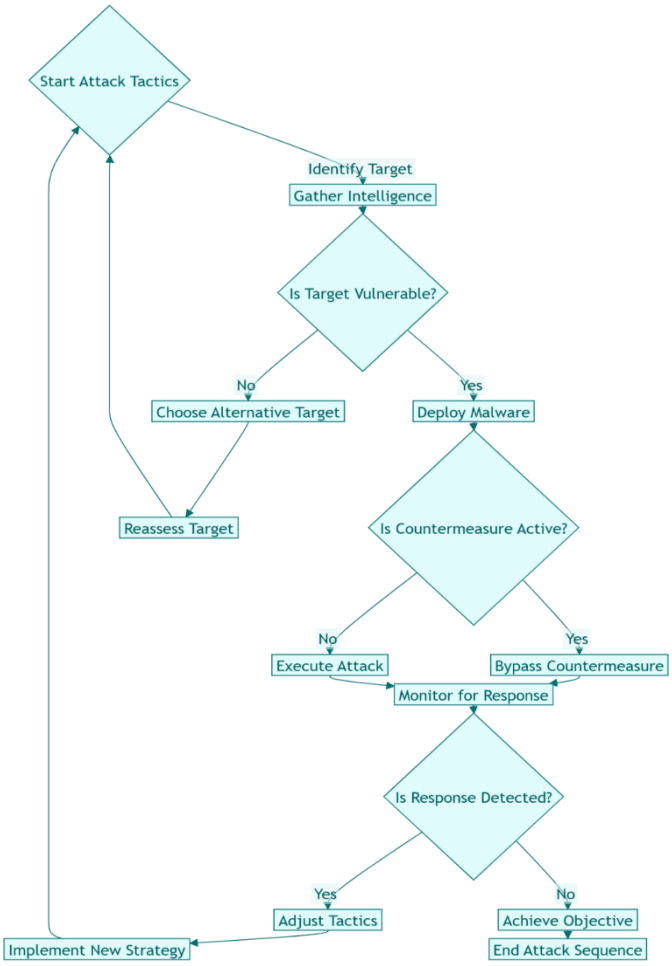

Figure 5: The sequence of steps for executing attack tactics.

Attackers typically deploy a diverse set of tactics to compromise the supply chain, sometimes as isolated incidents and other times as components of more sophisticated, multi-faceted attacks (Zhang & Thing, 2021; Gilbert & Gilbert, 2024l). Recognizing these methods is essential for organizations to accurately assess the threats they face and to develop robust defensive strategies (Gilbert & Gilbert, 2024m). Presently, many large organizations tend to deprioritize supply chain defenses within their broader cybersecurity frameworks (Singh et al., 2019; Gilbert & Gilbert, 2024i). However, as the understanding of these techniques and their potential impacts deepens, the imperative to defend against them is expected to rise (Gilbert & Gilbert, 2024k). Effective mitigation of supply chain attacks whether at a national or enterprise level, is particularly challenging, given that much of the security and resilience of the supply chain rests with external suppliers (Aljohani & Almutairi, 2024; Gilbert & Gilbert, 2024j). In

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

many cases, organizations are simply assemblers of systems and devices, relying on products and services provided by multiple vendors.

This flowchart details the iterative and dynamic nature of a cyber-attack, with decision points on the vulnerability of the target, countermeasures in place, and responses to the attack. The process involves constant adjustment and evaluation of tactics to ensure the success of the attack.

3.1. Software Integrity Verification

The emphasis on ensuring supply chain security during software development has often been diluted and misunderstood. A critical issue arises when trust is inadvertently extended to untrusted code, with the most significant risk stemming not from the code itself but from the individuals who sign it, implement changes, and the organizations they represent (Khan, 2023; Gilbert & Gilbert, 2024h). Essential security controls are frequently absent, leaving systems vulnerable to covert software updates injected by criminal or espionage activities, a vulnerability that recent military software supply chain incidents have starkly highlighted (Shahzad & Lu, 2023; Gilbert & Gilbert, 2024g).

If an assailant is able to jeopardize the integrity of the software compilation and build procedure, the security of all in-house developed software is called into question, with comparable dangers extending to open-source software that is not built internally (Wu, Duan and Ni, 2024; Kwame, Martey and Chris, 2017). Presently, there is a notable lack of robust software integrity verification mechanisms within the supply chain, both for developers and end users (Falade, 2024; Gilbert & Gilbert, 2025b). Although some commercial software publishers strive to enforce discipline in their build processes often aligning with standards such as ISO/IEC 27034, these efforts can sometimes be counterproductive (Gilbert & Gilbert, 2025a; Ried et al., 2021). By emphasizing the security of the build environment, purchasing decisions may be influenced by factors other than genuine supply chain security (Laux, Wachter & Mittelstadt, 2024). In practice, many commercial publishers rely primarily on digital signatures and post-release integrity metadata notifications to safeguard their software, which may not be sufficient to address the full spectrum of supply chain risks (Gilbert & Gilbert, 2024f).

3.2. Hardware Security Measures

A comprehensive strategy to mitigate hardware-specific attacks involves deploying heterogeneous multiprocessor architectures (Abilimi et al. 2015; Stojilović et al., 2023). In practice, this means integrating a mix of general-purpose, 3D-stacked, and commercial off-the-shelf processing elements that are optimized to function under challenging process variations while supporting Single-Instruction Multiple-Data (SIMD) operations (Abilimi, & Adu-Manu, 2013; Shantharama, Thyagaturu & Reisslein, 2020). By combining specialized processing units from different product lines into a stacked heterogeneous hierarchy, the system can effectively compartmentalize potential vulnerabilities including those exploited via statistical side-channel attacks (Gilbert & Gilbert, 2024e). Additionally, dynamically varying the processor's instruction set serves to obscure higher-level functionality, reducing the risk that any single component of the chip will become a reliable target for attackers (Veyette et al., 2022; Abilimi et al., 2013). Moreover, incorporating a chip-level personalization mechanism during manufacturing further enhances security by ensuring that each chip possesses unique attributes (Gilbert & Gilbert, 2024d).

Although software-based security measures remain essential, dedicated hardware solutions offer advantages that are difficult to replicate in software (Gilbert & Gilbert, 2024c; Cardellini et al., 2022). In particular, hardware implementations can enforce security policies with high efficiency (Chen et al., 2022; Gilbert & Gilbert, 2024b). The multi-SIMD design paradigm not only supports robust multi-threading—whether at the level of individual cores or across a multi-core architecture—but also delivers high throughput with relatively low complexity (Shakibhamedan et al., 2024; Gilbert & Gilbert, 2024a). These attributes are critical for maintaining computational security in environments where performance and resource efficiency are paramount.

TABLE 3: Security Measures Parameters compared

Security Measures Parameters	Software Integrity Verification	Hardware Security Measures
Effectiveness	7	8
Cost	6	7
Scalability	8	6
Complexity	6	8
Performance	5	9
Flexibility	7	5

In the table, Hardware Security Measures tend to be more effective, perform better, and are more complex, whereas Software Integrity Verification offers higher scalability and flexibility with lower complexity and cost. The choice between these two approaches depends on the specific needs and trade-offs of the system being protected.

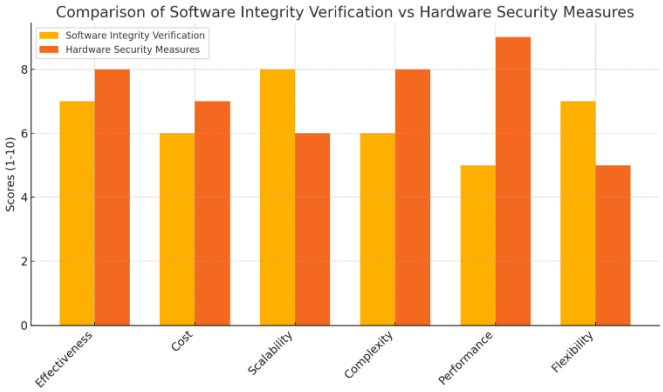

Figure 6: The Comparison of Software Integrity Verification Verses Hardware Security Measures.

The comparison between Software Integrity Verification and Hardware Security Measures shows their performance across key attributes. Software Integrity Verification, represented by the orange bars, excels in effectiveness and scalability but faces challenges in complexity, cost, and performance. On the other hand, Hardware Security Measures,

shown with yellow bars, perform well in terms of performance and complexity, though they slightly lag behind in scalability and flexibility. This chart clearly illustrates the differences between the two approaches in these areas, highlighting their respective strengths and limitations.

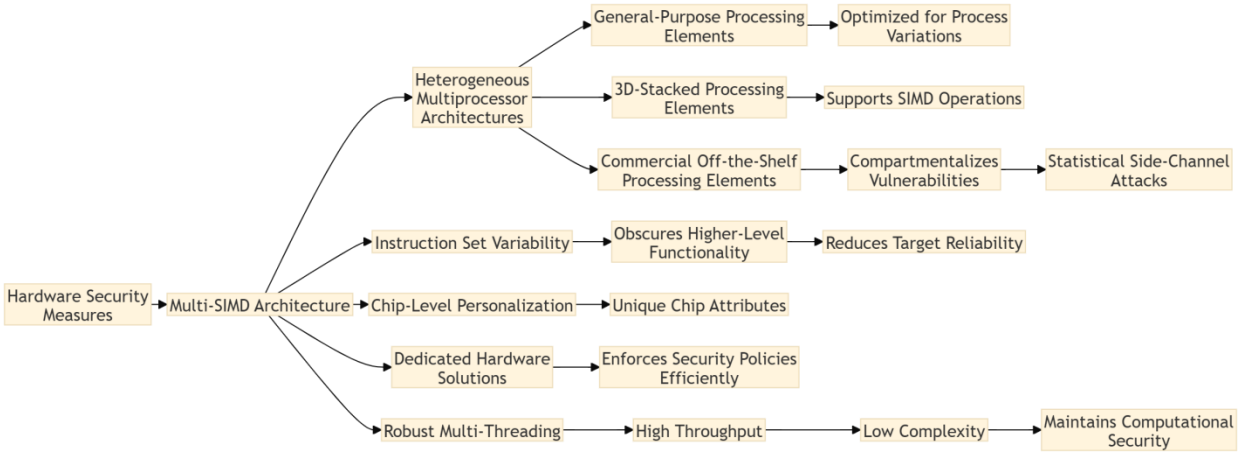

Figure 7: components and features of Hardware Security Measures **on** Multi-SIMD Architecture.

This diagram highlights how Hardware Security Measures**,** specifically Multi-SIMD Architecture, enhance system security by using heterogeneous multiprocessor architectures. These systems incorporate various processing elements, such as general-purpose, 3D-stacked, and commercial off-the-shelf components, all optimized for process variations and capable of supporting SIMD operations. The architecture helps mitigate statistical side-channel attacks by compartmentalizing vulnerabilities and obscuring higher-level functionality, which reduces the target's reliability. Additionally, Multi-SIMD Architecture offers benefits like instruction set variability, chip-level personalization, and the efficient enforcement of security policies, ensuring high throughput and low complexity. This approach provides robust multi-threading capabilities, which enhance performance while maintaining computational security and reducing vulnerabilities.

IV. Findings, Conclusions, Recommendations and Future Trends

4.1 Findings

- *Integration Vulnerabilities:* The study reveals that the integration of cyber-physical systems (CPS) and ultra-large-scale CPS (ULS-CPS) introduces significant vulnerabilities. These include cross-layer risks, insider threats, privacy issues, and collateral damage, all of which complicate the security landscape of supply chain networks.
- *Key Challenges Identified* - Three primary challenges were emphasized: *Third-Party Risks:* Inadequate security practices among external suppliers—especially when SMEs are involved—can expose sensitive data and create weak points in the network. *Complexity and Interconnectedness:* The inherent complexity of modern supply chains, where disruptions in one segment can cascade throughout the network, poses severe risks. Simplistic models often fail to capture the nuanced interdependencies among diverse participants. *Lack of Transparency:* Decision-making at critical nodes often lacks transparency, leading to imbalances and ad hoc practices that undermine equitable and efficient operations.
- *Assessment of Security Measures* -The evaluation of existing security techniques showed: *Software Integrity Verification:* Current practices (e.g., digital signatures and build process controls) may not be comprehensive enough, especially when trust is extended to potentially untrusted code or signers. *Hardware Security Measures:* Approaches such as heterogeneous multiprocessor architectures and dynamic instruction set variations offer promise by compartmentalizing vulnerabilities and mitigating side-channel attacks, yet they too have limitations in the face of evolving threats.
- *Novel Metrics Development:* The research introduced new metrics to assess the robustness and resilience of supply chain networks. These metrics indicate that even minor degradations in network resilience can lead to substantial losses in overall value.
- *Cross-Disciplinary Insights:* The findings underscore the importance of integrating insights from transportation policy, network security, and supply chain management to develop a holistic understanding of the vulnerabilities and to strategize effective defenses.

4.2 Conclusions

- *Integrated Security Approach Required:* The research concludes that securing supply chain networks requires a holistic strategy that goes beyond isolated technical fixes. An integrated framework that combines technological innovations with strategic, cross-disciplinary risk management practices is essential for long-term resilience.
- *Balancing Flexibility and Security:* While flexible and dynamic supply chains offer competitive advantages, they also expose organizations to targeted attacks. Therefore, decision-makers must weigh the benefits of operational

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Securing Supply Chain Networks," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 223-234, 2025.

agility against the heightened risk of sophisticated, coordinated cyber-physical threats.

- *Importance of Continuous Risk Assessment:* Given the rapid evolution of threats—particularly with emerging technologies—the study emphasizes the need for ongoing monitoring, verification, and re-assessment of security protocols throughout the supply chain lifecycle.

4.3 Recommendations

- *Enhance Risk Management Practices:* Organizations should implement robust, continuous risk management strategies that include: Comprehensive monitoring and verification of trustworthiness across all supply chain layers. Strengthened controls for third-party access, especially for suppliers handling sensitive data.
- *Improve Software and Hardware Security Measures: Software:* Adopt more rigorous integrity verification mechanisms that extend beyond digital signatures to include stricter controls on the code build process and trusted code signers. *Hardware:* Leverage heterogeneous multiprocessor architectures and dynamic instruction set variations to obscure functionality and compartmentalize potential vulnerabilities.
- *Promote Cross-Disciplinary Collaboration:* Stakeholders are encouraged to pursue industry-led initiatives that bring together experts in transportation policy, cybersecurity, and supply chain management. This collaboration can foster the development of integrated frameworks and standard protocols to secure complex networks.
- *Increase Transparency in Decision-Making:* To mitigate risks associated with opaque practices, it is recommended that supply chain processes be standardized and made more transparent. Clear contractual agreements and standardized protocols can help balance power among network participants and enhance overall trust.

4.4 Future Trends

- *Refinement of Novel Metrics:* Future research should focus on refining the proposed metrics for measuring network robustness and resilience. Validating these metrics through empirical studies can help quantify the real-world impact of security degradations.
- *Emerging Technological Impacts:* With technologies such as mass 3-D printing and photonic machining potentially decentralizing supply chains, further exploration is needed to understand how these innovations will affect vulnerability and security dynamics.
- *Sophisticated Modeling of Supply Chain Dynamics:* There is a growing need for advanced models that accurately capture the intricate interdependencies and dynamic interactions within global supply chains. Such models would better predict how disruptions propagate and how to design more resilient systems.
- *Increased Emphasis on Cyber-Physical Integration:* As CPS and ULS-CPS become more integral to supply chain operations, future security frameworks must evolve to address the unique challenges posed by their integration with traditional physical processes.
- *Industry-Led Security Initiatives:* The study highlights the potential for industry-led collaborations to pioneer innovative security strategies. These initiatives are expected to play a critical role in setting new industry standards and shaping policy in the realm of supply chain security.

REFERENCES

1. Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., ... & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering, 102647.
2. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9.
3. Abilimi, C. A., & Adu-Manu, K. S. (2013). Examining the impact of Information and Communication Technology capacity building in High School education in Ghana. International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9.
4. Abilimi, C.A., Amoako, L., Ayembillah, J. N., Yeboah, T.(2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. International Journal of Engineering Research and Technology, 2(11), 50 - 59.
5. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November - 2013
6. Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. Applied Sciences, 11(12), 5585.
7. Aljohani, T., & Almutairi, A. (2024). A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods. Defence Technology.
8. Aslaner, M. (2024). Cybersecurity Strategies and Best Practices: A comprehensive guide to mastering enterprise cyber defense tactics and techniques. Packt Publishing Ltd.
9. Bhamra, R., Hicks, C., Small, A., & García-Villarreal, E. (2022). Value, product delivery strategies and operational performance in the medical technology industry. International Journal of Production Economics, 245, 108399.
10. Becklines, L. (2024). FAIDS: artificial intelligence developmental systems framework for predicting and preventing cyberattacks in supply chain networks.
11. Cardellini, V., Lo Presti, F., Nardelli, M., & Russo, G. R. (2022). Runtime adaptation of data stream processing systems: The state of the art. ACM Computing Surveys, 54(11s), 1-36.
12. Can, C. M. (2024). Small power strategies under great power competition. International Politics, 61(2), 296-321.
13. Chen, W., Wang, Y., Xu, Y., Gao, C., Liu, C., & Zhang, L. (2022). A framework for neural network architecture and compile co-optimization. ACM Transactions on Embedded Computing Systems, 22(1), 1-24.
14. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.
15. Elahi, M., Afolaranmi, S. O., Martinez Lastra, J. L., & Perez Garcia, J. A. (2023). A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment. Discover Artificial Intelligence, 3(1), 43.
16. El-Kady, A. H., Halim, S., El-Halwagi, M. M., & Khan, F. (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety and Environmental Protection, 173, 384-413.
17. Falade, P. V. (2024). Investigating the security and privacy issues in ChatGPT usage and their impact on organisational and individual security. Int. J. Sci. Res. in Multidisciplinary Studies, 10(3).

18. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's The Road. English Journal, Volume 102, Issue Characters and Character, p. 40 - 47. https://doi.org/10.58680/ej201220821.
19. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. The Educational Forum, 83(1), 60–74. https://doi.org/10.1080/00131725.2018.1505017.
20. Gilbert, C. (2021). Walking the popular education spiral - an account and analysis of participatory action research with teacher activists. Educational Action Research, 30(5), 881–901. https://doi.org/10.1080/09650792.2021.1875856
21. Gilbert, C. (2022). Making the Invisible Visible: Professional Development to Support Teacher Activism. Kappa Delta Pi Record, 58(1), 14–19. https://doi.org/10.1080/00228958.2022.2005426
22. Gilbert, C. & Gilbert, M.A.(2024a). Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584.
23. Gilbert, C. & Gilbert, M.A.(2024b). Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816
24. Gilbert, C. & Gilbert, M.A.(2024c). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges. Global Scientific Journals.ISSN:2320-9186,12(9),427-441.
25. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. International Journal of Scientific Research and Modern Technology, 3(9), 9-9.
26. Gilbert, C. & Gilbert, M.A.(2024e). Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN: 2349-5162, Vol.11, Issue 10, page no.b299-b313.
27. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024, Volume 9, Issue 4, pp. 95-106.
28. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. International Journal of Scientific Research and Modern Technology, 3(10). https://doi.org/10.38124/ijsrmt.v3i10.54
29. Gilbert, C., & Gilbert, M. A. (2024h). Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.
30. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.
31. Gilbert, C. & Gilbert, M.A. (2024j). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation. International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.
32. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.
33. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. International Research Journal of Advanced Engineering and Science, 9(4), 205–219.
34. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. International Journal of Research Publication and Reviews, 5(11), 889–907. https://www.ijrpr.com
35. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. International Journal of Research and Innovation in Applied Science (IJRIAS), 9(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013
36. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. International Journal of Research Publication and Reviews, 5(11), 3235-3256. https://www.ijrpr.com.
37. Gilbert, C., & Gilbert, M. A. (2024p). Cryptographic Foundations And Cybersecurity Implications Of Blockchain Technology. Global Scientific Journals, ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com
38. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. International Research Journal of Advanced Engineering and Science, 9(4), 238–251.
39. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. International Journal of Scientific Research and Modern Technology, 3(11). https://doi.org/10.38124/ijsrmt.v3i11.76
40. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. International Journal of Scientific Research and Modern Technology, 3(11). https://doi.org/10.38124/ijsrmt.v3i11.77
41. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. International Journal of Research Publication and Reviews, 5(12), 507–533. https://www.ijrpr.com
42. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. International Journal of Research Publication and Reviews, 5(12), 1174–1191. Retrieved from www.ijrpr.com
43. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. International Journal of Research Publication and Reviews, 5(12), 1149–1173. Retrieved from www.ijrpr.com
44. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. Global Scientific Journal, 12(12). Retrieved from www.globalscientificjournal.com
45. Gilbert, C., & Gilbert, M. A. (2024x). Investigating the challenges and solutions in cybersecurity using quantum computing and cryptography. International Research Journal of Advanced Engineering and Science, 9(4), 291–315.
46. Gilbert, C., & Gilbert, M. A. (2024y). The integration of blockchain technology into database management systems for enhanced security and transparency. International Research Journal of Advanced Engineering and Science, 9(4), 316–334.
47. Gilbert, C., & Gilbert, M. A. (2025a). Artificial intelligence (AI) and machine learning (ML) for predictive cyber threat intelligence (CTI). International Journal of Research Publication and Reviews, 6(3), 584–617. http://www.ijrpr.com
48. Gilbert, C., & Gilbert, M. A. (2025b). Continuous user authentication on mobile devices. International Research Journal of Advanced Engineering and Science, 10(1), 158–173.
49. Gilbert, C., & Gilbert, M. A. (2025c). Patterns and vulnerabilities of cryptocurrency-related cybercrimes. Global Scientific Journal, 13(3), 1950-1981. https://www.globalscientificjournal.com
50. Gilbert, C., Gilbert, M. A., Dorgbefu, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025). Enhancing detection and response using artificial intelligence in cybersecurity. *International Journal of Multidisciplinary Research and Publications (IJMRAP), 7*(10), 87-104.
51. Gilbert, C., & Gilbert, M. A. (2025d). *Data encryption algorithms and risk management*. *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS), 14*(3), 479–507. https://doi.org/10.51583/IJLTEMAS.2025.140300054
52. Gilbert, C., Gilbert, M. A., & Dorgbefu Jnr, M. (2025a). *Secure data management in cloud environments*. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, 10(4), 25–56. https://doi.org/10.51584/IJRIAS.2025.10040003
53. Gilbert, C., Gilbert, M. A., & Dorgbefu Jnr, M. (2025b). Detection and Response Strategies for Advanced Persistent Threats (APTs). *International Journal of Scientific Research and Modern Technology, 4*(4), 5–21. https://doi.org/10.38124/ijsrmt.v4i4.367

54. Gilbert, C., & Gilbert, M. A. (2025e). Impact of General Data Protection Regulation (GDPR) on data breach response strategies (DBRS). *International Journal of Research and Innovation in Social Science (IJRISS)*, *9*(14), ***760–784***. https://doi.org/10.47772/IJRISS.2025.914MG0061
55. Gilbert, C., & Gilbert, M. A. (2025f). Algorithmic approaches to intrusion detection systems (IDS) using graph theory. *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, *7*(11), 109–125.
56. Gilbert, C., & Gilbert, M. A. (2025g). Homomorphic encryption algorithms for secure data computation. *International Research Journal of Advanced Engineering and Science*, *10*(2), 148–162.
57. Gilbert, C., & Gilbert, M. A. (2025h). Exploring Secure Hashing Algorithms for Data Integrity Verification. International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 7, Issue 11, pp. 373-390, 2025.
58. Gilbert, M.A., Oluwatosin, S. A. & Gilbert, C. (2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.
59. Gilbert, M.A., Auodo, A. & Gilbert, C. (2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.
60. Graefrath, M. S. (2023). Power Vacuums in Great Power Politics: the Consequences of Retrenchment and Collapse. University of Notre Dame.
61. Hasan, M. K., Alkhalifah, A., Islam, S., Babiker, N. B., Habib, A. A., Aman, A. H. M., & Hossain, M. A. (2022). Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wireless Communications and Mobile Computing, 2022(1), 9065768.
62. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications, 209, 103540.
63. Habibi, F., Chakrabortty, R. K., Abbasi, A., & Ho, W. (2025). Investigating disruption propagation and resilience of supply chain networks: interplay of tiers and connections. International Journal of Production Research, 1-23.
64. Kim, D. J. (2022). Compound Containment: A Reigning Power's Military-Economic Countermeasures against a Challenging Power (p. 212). University of Michigan Press.
65. Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115, 171-187.
66. Kumar, A., Liu, R., & Shan, Z. (2020). Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. Decision Sciences, 51(1), 8-37.
67. Kumar, C., Marston, S., & Sen, R. (2020). Cyber-physical systems (CPS) security: state of the art and research opportunities for information systems academics. Communications of the Association for Information Systems, 47(1), 36.
68. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. Communications on Applied Electronics, 7(7), 8-13.
69. Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. Regulation & Governance, 18(1), 3-32.
70. Liebowitz, J. (2019). Building organizational intelligence: A knowledge management primer. CRC press.
71. Lim, K. Y. H. (2023). Graph-enabled digital twins for intelligent product lifecycle management: a multi-dimensional approach to design, manufacturing, and supply chain transformation.
72. Lynberg, L., & Deif, A. (2023). Network effects in blockchain and supply chain: a theoretical research synthesis. Modern Supply Chain Research and Applications, 5(1), 2-27.
73. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. Comput. Eng. Intell. Syst, 4, 50-57.
74. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. International Journal on Computer Science and Engineering (IJCSE), 760-769.
75. Rosado, D. G., Santos-Olmo, A., Sánchez, L. E., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2022). Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. Computers in Industry, 142, 103715.
76. Ried, L., Eckerd, S., Kaufmann, L., & Carter, C. (2021). Spillover effects of information leakages in buyer–supplier–supplier triads. Journal of Operations Management, 67(3), 280-306.
77. Shakibhamedan, S., Aminifar, A., Vassallo, L., & TaheriNejad, N. (2024, July). Harnessing approximate computing for machine learning. In 2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (pp. 585-591). IEEE.
78. Shahzad, U., & Lu, C. (2023). The Effect of Zero Trust Model on Organizations.
79. Shifrinson, J. (2020). The rise of China, balance of power theory and US national security: Reasons for optimism?. Journal of Strategic Studies, 43(2), 175-216.
80. Sheikh, Z. A., Singh, Y., Singh, P. K., & Ghafoor, K. Z. (2022). Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. Computer Communications, 193, 302-331.
81. Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing, 75, 4543-4574.
82. Stojilović, M., Rasmussen, K., Regazzoni, F., Tahoori, M. B., & Tessier, R. (2023). A visionary look at the security of reconfigurable cloud computing. Proceedings of the IEEE, 111(12), 1548-1571.
83. Tahmasebi, M. (2024). Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. Journal of Information Security, 15(2), 106-133.
84. Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of IoT in boosting supply chain transparency and efficiency. Magna Scientia Adv. Res. Rev., 12(1), 178-197.
85. Vaidya, R. (2019). Cyber security breaches survey 2019. Department for Digital, Culture, Media and Sport, 66.
86. Veyette, M. J., Aylor, K., Stafford, D., Herrera, M., Jumani, S., Lineberry, C., ... & Jenkins, M. (2022). Ai/ml for mission processing onboard satellites. In AIAA SCITECH 2022 Forum (p. 1472).
87. Vyas, N., Dasgupta, D., & Sošic, G. (2024). Supply Chain Network Design: How to Create Resilient, Agile and Sustainable Supply Chains. Kogan Page Publishers.
88. Wu, X., Duan, R., & Ni, J. (2024). Unveiling security, privacy, and ethical concerns of ChatGPT. Journal of Information and Intelligence, 2(2), 102-115.
89. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A. (2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. Journal of Engineering, Computers & Applied Sciences (JEC&AS), 2(7).
90. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment.
91. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b). Automatic Biometric Student Attendance System: A Case Study Christian Service University College. Journal of Engineering Computers & Applied Sciences, 2(6), 117-121.
92. Yeboah T. & Abilimi C.A. (2013). Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, "2(11).
93. Zhang, L., & Thing, V. L. (2021). Three decades of deception techniques in active cyber defense-retrospect and outlook. Computers & Security, 106, 102288.
94. Zekhnini, K., Cherrafi, A., Bouhaddou, I., Benghabrit, Y., & Garza-Reyes, J. A. (2021). Supply chain management 4.0: a literature review and research framework. Benchmarking: An International Journal, 28(2), 465-501.

95. Zhang, L., & Thing, V. L. (2021). Three decades of deception techniques in active cyber defense-retrospect and outlook. Computers & Security, 106, 102288.