Machine learning techniques were applied to different classification algorithms to train on a dataset for performance accuracies and threat prediction based on the CSC resilience design principles. Some of the technique used include logistic regression, decision tree, Naive Bayes and random Forest, Neural Network classification algorithm were analyzed to predict the result. The threat was finally mapped with some familiar attacks to draw inferences to improve resilience on critical assets.

Contribution to Knowledge: At the end the study was able to improve cyber supply chain system resilience by understanding and predicting the threats. The result of the findings shows a 70% performance accuracy for the threat prediction with cyber resilience design principles that focus on critical assets and reduce the threat.

7. Resilient Chain: AI-Enhanced supply Chain Security and Efficiency Integration [11]:

Objectives: The study aim examines the current state of AI integration across U.S supply chain sector while focusing on key areas such as real time tracking, cost optimization and risk management.

Methodology: The study used the contingency theory approach to explain the use of AI-Enhanced supply chain security model factored through resilient chains. The contingency approach states that there is no universal approach to organizational management and so effective strategies depend on the specific context and circumstances. A mixed method approach which utilizes inferential and descriptive analyses was adopted to uncover insight and trend of AI role in supply chain. A questionnaire survey of about 281 company managers was carried out using random selection to select the participant with the goal of examining the current state of AI integration across the U.S supply chain sector.

Contribution to Knowledge: The study show exposed the pivotal role of AI in strengthening the supply chain security system in the United State the result of the research carried out provide valuable insight for organization seeking to explore the complexities of modern supply chain management.

8. An efficient web Authentication Mechanism Preventing Man-in-the-Middle attacks in Industry 4.0 supply chain [12]:

Objectives: To propose an efficient TLS-based authentication mechanism that can resist against MITM attacks in web application.

Methodology: The TLS-based authentication mechanism is based on the SISCA mechanism, and it relies on Channel ID-based authentication and server invariance.

Contribution to Knowledge: The study was able to achieve browser and server's identity confidentiality and resistance against MITM attacks. Their proposed model also helps to reduce the communication overhead by 50%.

Limitation: The stated that future work would require the implementation of the model between a client and a server running on two different machines interconnected over the internet. And, to adopt the model to provide lightweighted authentication along with resistance against MITM attack in communication industry.

9. Design and Evaluation of Privacy preserved supply chain system based on public blockchain [13]:

Objectives: To propose a method for preserving privacy while securing traceability of product in the supply chain system that uses PBC.

Methodology: The study proposed a method for preserving the privacy of distribution information by extending POMs. The method uses a public key to encrypt blockchain address of the product manufacturer. It consists of manufacturer manager Contract (MMC) for managing product distribution and verifier contract (VC) for verifying a proof based on the zero-knowledge proof. The model was implemented on Ethereum platform.

Contribution to Knowledge: The proposed method helps to preserve the privacy of supply chain by concealing the distributed information through encryption. This model also helps to ensure distribution within a supply chain while also hiding their blockchain address using zero-knowledge proof authentication.

Limitation: The proposed method only assumes the distribution of a single product without modification therefore it could not be applied to the assembly and disassembly of a finished product.

10. Research on Supply Chain Financial Risk Prevention Based on Machine Learning [14]:

Objectives: To propose an AI based corporate financial risk prevention model

Methodology: The proposed model to prevent financial risk in supply chain that includes data preprocessing stage, feature selection stage based on CGOA, and data classification based on SVM, and parameter classification based on SMA. Python was used to simulate the function of the corporate business financial risk prevention model.

Contribution to Knowledge: The proposed model CGOA-SVM-SMA from result of the experiment based on overall accuracy performance, shows it has a better decision-making effect over F-Score and TNR.

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

Limitation: The study did not consider the influence of outliers as companies with missing data were removed during the preprocessing period. And so, they recommend that future study should include a method that can detect outliers to the model.

11. An Efficient web Authentication Mechanism Preventing Man-in-the-Middle attacks in Industry 4.0 supply chain [15]:

Objectives: To propose an efficient TLS-based authentication mechanism that can resist against MITM attacks in web application.

Methodology: The TLS-based authentication mechanism is based on the SISCA mechanism, and it relies on Channel ID-based authentication and server invariance.

Contribution to Knowledge: The study was able to achieve browser and server's identity confidentiality and resistance against MITM attacks. Their proposed model also helps to reduce the communication overhead by 50%.

Limitation: The stated that future work would require the implementation of the model between a client and a server running on two different machines interconnected over the internet. And, to adopt the model to provide lightweighted authentication along with resistance against MITM attack in communication industry.

12. Cybersecurity Attack Detection Model Using Machine Learning Techniques [16] :

Objectives: the study aim to create an effective IDS based on machine learning and feature selection techniques

Methodology: The study proposed an effective network intrusion detection system that is based on machine learning and feature selection techniques. Performance measures were carried out based on four different techniques of machine learning which are RF, KNN, SVM and DT and used to predict intrusion detection.

Contribution to Knowledge: At the end of the study experiment, the proposed methodology achieved a great result as the RF technique achieved an accuracy of 99.72% as compared to other techniques.

Limitations: The study only focuses on whether traffic is malicious or benign and not on authenticating who or what accesses the network, and the author advised that future work be developed to classify the different types of cyber security.

13. Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration [18]:

Objectives: The study aim examine the current state of AI integration across U.S supply chain sector while focusing on key areas such as real time tracking, cost optimization and risk management.

Methodology: The study used the contingency theory approach to explain the use of AI-Enhanced supply chain security model factored through resilient chains. The contingency approach states that there is no universal approach to organizational management and so effective strategies depend on the specific context and circumstances. A mixed method approach which utilizes inferential and descriptive analyses was adopted to uncover insight and trend of AI role in supply chain. A questionnaire survey of about 281 company managers was carried out using random selection to select the participant with the goal of examining the current state of AI integration across the U.S supply chain sector.

Contribution to Knowledge: The study show exposed the pivotal role of AI in strengthening the supply chain security system in the United State the result of the research carried out provide valuable insight for organization seeking to explore the complexities of modern supply chain management.

4. Motivation

The ever-increasing complexity and interconnectedness of supply chain activities has created a significant vulnerability to cyberattacks. Supply chain attack can be very detrimental as attackers can infiltrate organizations network undetected for a long period of time waiting dormant for the best time to carry out defect evil act ranging from data breaches, operational disruption, and reputational harm. The Complexity of an organization interconnected networks with their third parties (Vendors) inculcated into this same network cannot be entirely monitored by the organizations and so it is important that an organization put in place strict and comprehensive security measures to defend against compromises Some of the way in which supply chain can be attack include compromising software updates, inculcating malicious codes in hardware or firmware, watering hole attacks in which an attack compromise website frequently used by a specific vendor or organization, social engineering attack against vendors, exploiting vendors API, intercepting or hijacking communication through man-in-the middle attack etc.

Conventional security approaches are no longer enough to hold off these attacks as it often relies on perimeter defense, a defense technique in which cyber attackers can now bypass to gain access to an organization domain mostly through a third-party vendors link and carry out their evil act. There is need to put strict security measures in place to overcome the blind spot and vulnerabilities within the network. and so, we proposed the adoption of a zero-trust

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

framework to mitigate against cyber supply chain attack.

5. Proposed System Designed

The proposed methodology for mitigating against supply chain attack is centered around using AI-powered zero trust framework to address some of the challenges in conventional network security and in improving some of the limitations encountered by the previous author such as mitigating against unauthorized identity and access management to devices, network security and data breaches.

What then is Zero Trust?

According to the National Institute of Standard and Technology (NIST), the Zero Trust Security Framework is defined as a set of cybersecurity principles that shift defenses from static, network-based perimeters to focus on users, assets, and resources. This approach ensures that no implicit trust is granted to assets or user accounts based solely on their physical or network location, but authentication and authorization are required for every access request, regardless of where the request originates.[19]

5.1. Architecture Flowchart

The architectural flowchart is a visual representation of how the zero-trust system is developed from the idea conception to the final implementation and usage. The flowchart provides an overview of the system's functional elements, their interactions, and the flow of data or control between them (see Figure 1).

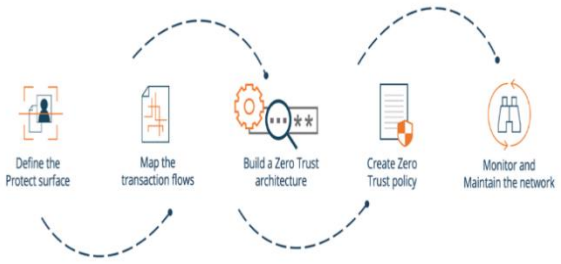

Figure 1: Architecture flowchart

The Architecture flow chart Explained

1. Define the Protect surface: this phase involves the identification of all the resources within the network that can be threatened and so need protection from attack whatsoever. Some of the resources include data, applications, servers, user devices etc. Figure 2 shows a pseudo network surface that requires protection, and the entities connected to it.

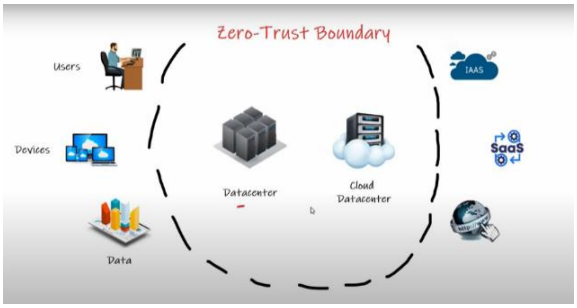

Figure 2: Network Surface Area Requiring Protection

Threat Associated with Supply Chain Activities of An Organization

In defining the surface to protect involves identifying areas that are threat susceptible, this is to understand the best zero trust principle and technique to apply in mitigating the possibility of such attack. Some of the Threat that are associated with the supply chain activities of an organization:

i. *Third Party Vulnerabilities* in supply chain can occur in different ways which include attackers using different means such as phishing, social engineering or combination of different form of attack mode to obtain suppliers credentials to gain access to an organization network environment, also a supplier to an organization can have weak security practices due to limited resources such as use of outdated software or lack of expertise, which can be exploited by attackers to gain access to the main organization network environment being the main target. An organization inability to have full visibility into their third party's security postures will make it quite difficult to identify and address the potential risks within the supply chain link. This is one major reason why an organization needs to have their own means of preventing threat from any of their third parties gaining access into their own domain.

ii. *Network Disruption / Denial of Service Attack* is to disrupt the normal flow of organization communication within its network and these attacks are mostly carried out through Denial of service (DOS) or DDOS attacks which is an attack involving overwhelming the network with excessive amount of traffic making the service unavailable to the authorized users or even prevent some critical services on the network from functioning correctly. An organization network can attack through its network of Third parties including suppliers and distributors. DOS or DDOS as simple as the English sound when carried out by an attacker can run an organization to a heavy lose. There are several ways through

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

which DOS attack can be exhibited. It includes Volume-Based Attack, protocol attacks, application layer attacks.

iii. *Physical Security Gap* focus on what goes on the network much more than the physical devices, while cyber vulnerabilities are an important area of focus in securing our supply chain, overlooking the physical and infrastructure security vulnerabilities such as weak security perimeter, compromised access control, tailgating and piggybacking can create significant impact on ensuring the safety of all networks.

iv. *Data Breaches / Insecure Data Handling* situation report of some third party / vendors storing sensitive data on unencrypted server/ devices, or organizations receiving mail and data through unencrypted channels such as email or FTP or even third parties not having data loss prevention solutions in place to protect against data breach or loss could lead to serious financial or reputation damage to an organization.

2. *Map the Transaction flow*: This phase focused on determining how data and access request flow within the network. It involves identifying the users, applications, resources accessing the network and which communication path is being used by these entities. This phase helps us to locate and understand vulnerabilities hence being able to define the type of control policy to implement for each resource and communication path. Figure 3 shows the flow of

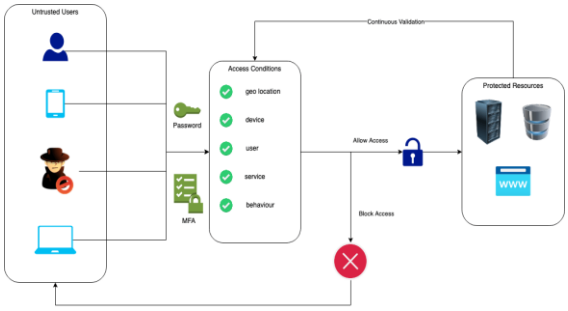

Figure 3. Access Request Communication Path within the Network

access request being made by different entities into a network and how this request should either be granted or denied based on parameters such as location, device used, pattern of request, and the user making the request. All the above parameters are necessary to know the type of zero trust policy to adopt in the model.

3. *Build Zero Trust Architecture*: The main target of securing a network environment is to uphold the three Core principles of security which are Confidentiality, Integrity of Information and Availability of services. These principles have a high chance of being upheld by zero trust framework. As stated early, the core principle of zero trust Architecture is to ensure that only authenticated and authorize user can access the network environment and in ensuring this principle are carried out, there is need to have a strong authentication in place at the endpoints zone (the entry point) this is to ensure only the right user/ device can access just what they need to access and nothing more.

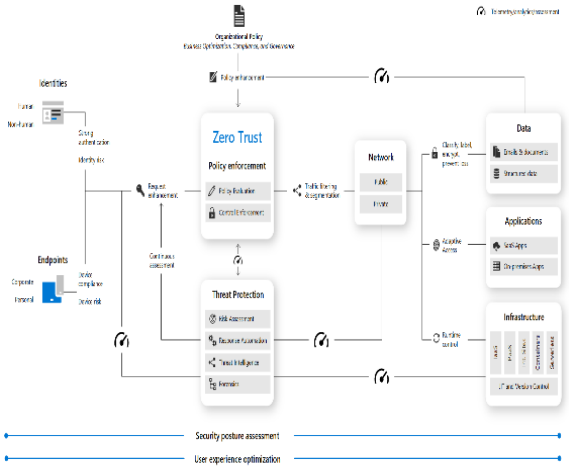

Figure 4. Zero Trust Framework Architecture.[8]

In the Zero trust Framework, the whole communication area is segmented into different areas, by employing the Micro-segmentation policy this is to prevent access of entities into unauthorized areas. In protecting our supply chain environment, we adopt the Microsoft Azure Zero trust framework with the diagram below (see Figure 4). The adopted framework encompasses three important key criteria which include: Identity and Access management, using (multi-factor authentication, Micro-segmentation), data Protection, and finally continuous protection and monitoring of the network activity. Some Key Components of the Zero Trust framework include:

i. *Identity and Access Management (IAM)* - This involves the Centralized management of all user identities and access privileges. Users' identity and authorization based on predefined policies are carried out here. It includes strong authentication mechanisms (e.g., multi-factor authentication), continuous monitoring of user behavior and privileges.

ii. *Network Segmentation* - This involves dividing the network into smaller, isolated segments. This is to restrict lateral movement within the network and access to specific resources thereby enforcing the least privileged access principles.

iii. *Data Encryption* - This Involve Encrypting data at rest and in transit to protect against unauthorized

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

access with the use of strong encryption algorithms and protocols data and information can be well secured from unauthorized access.

iv. *Continuous Monitoring and Analytics* - Real-time monitoring of network traffic and user behavior such as analyzing data for anomalies and security threats and implementing security information and event management (SIEM) solutions to foster strict security within the network. This phase involves network data collection and analysis to identify anomalies and security threats within the network.

v. *Policy Enforcement* - Enforcing strict access control policies based on user identity, role, and context and dynamically adjusting policies based on risk assessments to restrict access to resources based on user identity and context.

4. *Create Zero Trust Policy*: A Zero Trust policy is a set of rules and guidelines that define how the zero-trust system will operate. It defines the principles, mechanisms, and procedures for implementing Zero Trust architecture. It involves creating protocols and principles governing access of any entity to the network environment within the zero-trust framework. The policy includes users' access permission based on the least privilege conditions such as MFA requirement, data access and sharing restriction policy based on entity roles within the network, and security protocols for communication within the network. Key considerations to put in place when creating polices include:

i. *Risk Assessment*: There is a need to conduct a thorough risk assessment to identify potential threats and vulnerabilities.

ii. *Compliance*: Ensure that the policy complies with relevant regulations and industry standards.

iii. *User Experience*: Balance security requirements with the need for positive user experience.

iv. *Scalability*: Design the policy to be scalable and adaptable to future changes.

The core principles of the zero-trust framework.

- *Never Trust, Always Verify*: This implies that every request made to a network or within the network regardless of its origin must be verified before access is granted.
- *Least Privilege Access*: This implies that users, software, and devices are granted only the minimum level of access required to carry out their task. This is to minimize potential damage.
- *Micro-segmentation*: This is the practices of breaking up security perimeters into smaller isolated segment to maintain different access for different part of the network. This help to reduce the rate of lateral movement of attackers within the network even if they gain access to a specific device or system.
- *Continuous Verification*: This involves continuous evaluation and reauthentication of access request throughout a session at every point and not just at the login point as opposed to the one-time authentication of the conventional security method. This is to ensure that compromised credentials or stolen tokens cannot be used for authorised access.
- *Identity and Device Access Management*: This principle involve the use of strong authenticating techniques such as multifactor authentication (MFA) to verify users' identities at every access request point and the use of device posture check to ensure devices meet security standard before access are granted.
- *Data Security*: This focus on protecting of data rather than relying solely on perimeter security. It involves encrypting data in both rest and transit state to protect it against unauthorised access, even if an attacker breaches the network perimeter.

Elements of Zero Trust Policy Include:

- *Authentication*: Require strong passwords, MFA, and biometric authentication for sensitive resources.
- *Authorization*: Implement RBAC to assign appropriate privileges based on user roles and responsibilities.
- *Data Encryption*: Encrypt all data at rest and in transit using AES-256 or stronger encryption.
- *Network Micro-segmentation*: Dividing the network into separate zones for different functions (e.g., production, development, DMZ).
- *Firewall Rules*: Implementation of strict firewall rules to control network traffic.
- *Intrusion Detection and Prevention (IDP)*: Deploy IDP systems to detect and prevent unauthorized access.
- *Regular Security Assessments*: Conducting regular vulnerability scans and penetration testing.

Implementation of Zero Trust Architecture in A Supply chain environment

Migration to zero trust framework by an organization will likely take a while as the path to zero trust is an incremental process and for a zero-trust framework to coexist fully with a non-zero trust environment, an organization needs to have detailed

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

knowledge of its assets both physical and virtual, entities accessing the environment, and business processes going on within the environment. with ensuring that common elements such as ID and access management, device configuration and management, segmentation of the network environment, and event logging.

5.2. The Role of AI in Zero Trust System

Achieving a zero-trust security environment requires the use of advanced technology that can evaluate systems and processes in real time, assess network activity, and determine risks associated with the behavior of the system and processes. In a zero-trust system in which every access needs to be verified and authenticated before being granted, the main role of AI is to provide real time threat assessment while ensuring that only authorised users and devices are granted access. AI ability to detect threats and automate response to this threat is of high importance within the zero-thrust system. The benefits of AI integration into a Zero Trust Framework in enhancing supply chain security:

i. *Data Driven Risk Assessment* - Integration of AI into the Zero trust framework can aid in analyzing large amounts of data from various sources such as vendor security report, threat intelligence, network traffic logs etc.in order to identify potential vulnerabilities that might emerge from third party's links.

ii. *Anomaly Detection* - AI can continuously monitor network activity and user behavior within the supply chain identifying subtle changes in patterns thereby enabling early detection of hidden threats.

iii. *Automated Threat Response* - AI-powered zero trust system can automate certain aspects of the incidence response process such as isolating compromised systems. This reduces the response time to threat incidence thereby minimizing the impact of cyberattacks. The benefits of AI-powered Zero-Trust Framework Over Traditional Frameworks are:

From the past we can deduce that Traditional security often finds it difficult to keep up with the evolving threats targeting supply chains systems nowadays, below are some of the benefits of AI-powered Zero Trust framework over traditional ones.

i. *Enhanced Threat Detection and Proactive Defense* - Traditional means of relying on perimeter defense against sophisticated attacks can be slow and liable to missing subtle threats. This shortcoming can be overcome by AI algorithms that continuously analyze vast amounts of data from different sources at reduced time.

ii. *Improved Risk Management and Resource Allocation* - Traditional risk assessment relies mostly on static data sometime not capturing dynamic datapoints, but AI-powered zero trust consider vast amount of datapoint and continuously learn from new information, which enable organization to prioritize security resources based on critical risk unlike traditional ones that focus on resolving immediate risk instead of long-term risk mitigation.

iii. *Faster Response Times and Damage Control* - With traditional system incidence response processes often involve manual analysis and decision making which can lead to delay in containing cyberattacks while with AI-powered zero trust, threat response automation can help to reduce the time it takes to isolate compromised systems and mitigate damages.

iv. *Scalability and Adaptability to Evolving Threats* - Traditional methods might find it difficult to adapt to the ever-increasing complexity and changes in supply chain networks but with AI ability to continuously retrain itself with new data allowing them to adapt to emerging threats.

v. *Improving Decision-making Efficiency* - Tradition -al security relies on limited data and human decision-making ability which can lead to poor decision making but with AI-powered Zero Trust Analytics ability to provide valuable insights into the supply chain security position, more informed security and resource allocation decisions can be made which in turn improve overall system performance.

6. Comparative Analysis of Supply Chain Security using Zero trust Framework and Traditional perimeter Framework

i. *Trust assumption* - in terms of trust, traditional perimeter security models operate on the assumption that everything inside the network perimeter is trustworthy therefore granting access to any entity within the premises while Zero Trust operates on the principle of "never trust, always verify" principle

ii. *Access Control* - In Traditional model access controls are often static and based on roles or groups, thereby making it difficult to adapt to changing user/group role while for zero trust, access control is dynamic based on continuous authentication thereby providing a more dynamic and responsive security posture.

iii. *Primary Focus* - Traditional perimeter security focuses on protecting the network from external threat therefore overlooking threat that gain access to the network while zero trust prevent against

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

both internal and external threat thereby strengthening the environment.

iv. *Network Micro-segmentation* - Traditional secure -ty is limited when it comes to segmentation unlike zero trust implementation that enables the division of the network into smaller isolated segments thereby reducing attack surface and limit lateral movement.

v. *Visibility* - Traditional security has limited visibility and lacks continuous monitoring while zero trust has more visibility and continuous monitoring and analytics.

vi. *Access Principle* - Traditional frameworks enable broad access within the system but with zero trust access is based on the least privilege.

vii. *Threat Detection* - Traditional perimeter security is reactive when it is based on detecting threat while zero trust is proactive and real time.

7. Conclusion

In conclusion, implementation and deployment of AI-powered Zero trust framework .in enhancing supply chain security is a gradual process rather than a wholesome replacement of infrastructure or processes. Organizations should seek to sequentially implement zero trust principles, process changes, and technology solutions to protect their environment. Most enterprises will continue to operate in a hybrid zero-trust/perimeter-based mode for a quite a period while continuing to invest in ongoing IT modernization through data risk assessment, proactive threat detection and automated response mechanism, businesses supply chain ecosystem can be more secured against cyber-attacks therefore engaging in smooth flow of business activities. To sum it all, it is essential for organizations to carefully assess their specific needs and develop a tailored Zero Trust strategy that aligns with their overall security objectives.

8. References

[1] Gillis A. S. (2023). Supply Chain Attack. “TechTarget Security”. Home and Vulnerabilities. https://www.techtarget.com/searchsecurity/definition/supply-chain-attack. (Access Date: 25 July 2024).

[2] Abou El Houda, Z. (2024). Cyber Threat 5 Actors Review. Cyber Security for Next-Generation Computing Technologies, 84.

[3] Avcı, İ., and Koca, M. (2023). Cybersecurity Attack Detection Model, Using Machine Learning Techniques. Acta Polytechnica Hungarica, 20(7), 29-44.

[4] Cheng, Y., Du, Y., Peng, J., Fu, J., and Liu, B. (2019). Research on identity authentication methods based on negative logic systems. In Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018, Revised Selected Papers 15 (pp. 3-15). Springer Singapore.

[5] Lee, J., Kim, J., Kim, I., and Han, K. (2019). Cyber threat detection is based on artificial neural networks using event profiles. Ieee Access, 7, 165607-165626.

[6] Sharma, S., and Routroy, S. (2016). Modeling information risk in supply chain using Bayesian networks. Journal of Enterprise Information Management, 29(2), 238-254.

[7] Yeboah-Ofori, A., Islam, S., and Brimicombe, A. (2019, May). Detecting cyber supply chain attacks on cyber physical systems using Bayesian belief network. In 2019 International conference on cyber security and internet of things (ICSIoT) (pp. 37-42). IEEE.

[8] Microsoft Azure. (2024). Zero-Trust Security. Guiding Principles of Zero Trust. https://learn.micro soft.com/en-us/azure/security/funddamentals/zero-tru st (Access Date: 23 July 2024).

[9] Khalid H. (2022). How to start with Zero trust Architecture roadmap. https://www.linkedin.com/pulse/how-start-zero-trust-architecture-roadmap-khal id-hussain/. (Access date: 23 July 2024).

[10] Yeboah-Ofori, A., Swart, C., Opoku-Boateng, F. A., and Islam, S. (2022). Cyber resilience in supply chain system security using machine learning for threat predictions. Continuity and Resilience Review, 4(1), 1-36.

[11] Chukwu, N., Yufenyuy, S., Ejiofor, E., Ekweli, D., Ogunleye, O., Clement, T., ... and Obunadike10, C. (2024). Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration. Int. J. Sci. Manag. Res, 7(03), 46-65.

[12] Esfahani, A., Mantas, G., Ribeiro, J., Bastos, J., Mumtaz, S., Violas, M. A., ... and Rodriguez, J. (2019). An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain. IEEE Access, 7, 58981-58989.

[13] Uesugi, T., Shijo, Y., and Murata, M. (2020). Short paper: Design and evaluation of privacy-preserved supply chain system based on public blockchain. arXiv preprint arXiv:2004.07606.

[14] Lei, Y., Qiaoming, H., and Tong, Z. (2023). Research on supply chain financial risk prevention based on machine learning. Computational Intelligence and Neuroscience. 2023(1), 6531154.

[15] Esfahani, A., Mantas, G., Ribeiro, J., Bastos, J., Mumtaz, S., Violas, M. A., ... and Rodriguez, J. (2019). An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain. IEEE Access, 7, 58981-58989.

[16] Avcı, İ., and Koca, M. (2023). Cybersecurity Attack Detection Model, Using Machine Learning Techniques. Acta Polytechnica Hungarica, 20(7), 29-44.

 | DOI: 10.20533/ijicr.2042.4655.2024.0155

[17] Sarah Gordon et Richard Ford. (2006). The Definition and Classification of Cyber crime. Journal in computer Virology 2:1 (2006):13-20.

[18] Chukwu, N., Yufenyuy, S., Ejiofor, E., Ekweli, D., Ogunleye, O., Clement, T., ... and Obunadike10, C. (2024). Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration. Int. J. Sci. Manag. Res, 7(03), 46-65.

[19] Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. DOI: 10.6028/NIST.SP.800-207. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420 (Access October 28 2024).

9. Acknowledgements

We are also grateful to the Infonomics Society for funding this publication. Their support has been instrumental in advancing research and dissemination of knowledge enhancement worldwide.