Educational Administration: Theory and Practice
2023, 29(2), 872-878
ISSN: 2148-2403
https://kuey.net/

Research Article

Enhancing Iot Device Security In Smart Supply Chains Challenges And Solutions

Dr. Syed Umar[1*], Jyothinadh Nadella[2], Ramu Mannava[3], Vinay Chowdary Dabbara[4], Dr.Ramesh Safare[5]

[1*]Professor, Department of CSE, HMKS&MGS College of Engineering, India. Umar332@gmail.com.
[2]Software Engineer, Verinon Technology Solutions. nadellajyothinadh@gmail.com
[3]Master's in Information Technology, Arkansas Tech University, Ramu.mannava1@gmail.com
[4]Master of Science Student, Dept. Cyber Security operations, Webster University. dabbaravinaychowdary@gmail.com
[5]Associate Professor, Faculty of Management Studies, Marwadi University, Rajkot, India.
ramesh.safare@marwadieducation.edu.in

Citation: Dr.Syed Umar, et.al (2023), Enhancing Iot Device Security In Smart Supply Chains Challenges And Solutions, *Educational Administration: Theory and Practice*, 29(2) 872-878
Doi: 10.53555/kuey.v29i2.9583

ARTICLE INFO

ABSTRACT

The integration of Internet of Things (IoT) devices into smart supply chains has revolutionized manufacturing and logistics by enabling real-time tracking, automation, and improved decision-making. Due to serious security flaws brought about by the growth of linked IoT devices, supply chains are now more vulnerable to assaults. In the context of smart supply chains, IoT device security poses unique challenges, including device heterogeneity, scalability constraints, data privacy concerns, and the potential for device manipulation. Given the decentralized and dynamic nature of IoT networks, we analyze existing security frameworks and highlight their shortcomings. Additionally, we suggest a multi-layered security strategy that incorporates cutting-edge encryption techniques, block chain, and edge computing to make IoT networks more resilient. This paper addresses these problems and offers practical security solutions in an effort to provide a roadmap for companies wishing to safeguard their IoT-enabled supply chains. This will guarantee reliability, secrecy, and data integrity in a world growing increasingly interconnected by the day.

Keywords: IoT Security, Smart Supply Chain, Device Authentication, Data Encryption, Endpoint Security, Secure Communication Protocols, Firmware Integrity, Network Segmentation.

1. INTRODUCTION

The Internet of Things, or IoT, is being quickly embraced by modern supply chains. It is transforming organizations by facilitating automation, real-time tracking, and more effective operations. However, because IoT devices serve as important touch points for cyber threats, this networked world also poses serious security dangers. Securing sensors, RFID tags, and smart meters—devices that are widely used in smart supply chains to track shipments, monitor inventories, and improve industrial processes—is essential to protecting the ecosystem as a whole.

The vulnerability of many IoT devices is inherent, which is problematic because they often lack robust security features, are difficult to update, and may operate in remote or unmonitored environments. These weaknesses give rise to potential cyber-attacks, such as supply chain interruptions, device manipulation, and data breaches. The availability, confidentiality, and integrity of supply chain operations are thereby ensured by securing IoT devices.

The main obstacles to improving IoT device security in intelligent supply chains are examined in this study, along with possible remedies to mitigate these dangers. We will examine how companies may strengthen their IoT security posture by leveraging advanced technologies like block chain, edge computing, and artificial intelligence in conjunction with strong encryption and authentication systems. Security of IoT devices is ultimately critical to safeguarding private information and building resilience and trust in the increasingly digitalized supply chain environment.

Device Authentication

An essential part of IoT network security is device authentication, especially in intelligent supply chains. As IoT devices—from sensors and actuators to RFID tags and connected machinery—become more and more common in supply chain operations, it is imperative to make sure that only authorized devices are able to connect to the network. This will lessen the likelihood of possible assaults, illegal access, and data breaches.

Because devices in an IoT-enabled supply chain frequently communicate with one another, cloud platforms, and other IT systems, device authentication is an essential step in ensuring system security and data integrity. In the absence of appropriate authentication, malevolent actors may be able to take over devices, alter data, or penetrate the larger network. Device authentication establishes trust between the devices and the systems they communicate with in this situation in addition to ensuring that the devices are authentic. In smart supply chains, IoT ecosystems are made up of a large number of devices, many of which have limited resources. This means that traditional, computationally intensive authentication methods are difficult for smaller or less powerful devices to employ. Keeping track of IDs across hundreds or even millions of devices can be challenging and time-consuming. So that only authorized devices are connected to the network, each device must have a secure identity that can be checked at each connection point.

Secure Communication Protocols

IoT devices continuously transmit data across networks in a smart supply chain, whether during transportation, within a factory, or between different supply chain stakeholders. Sensitive information including production procedures, shipment tracking information, and inventory levels are frequently included in this data. If security safeguards aren't in place, bad actors could intercept, change, or spoof this communication.

Often, IoT devices use a variety of networks, some of which may not be dependable, such as public WiFi, cellular networks, and even low-power networks like Lora WAN. These networks are susceptible to man-in-the-middle (MITM) attacks, replay assaults, and eavesdropping. Low-cost, low-power, and resource-restricted, many IoT devices in supply chains have constrained memory, bandwidth, and computing power. Because of this, it could be difficult to implement sophisticated security features (like end-to-end encryption) without making things slower or using up too much battery life. Different firms may produce IoT devices in a smart supply chain, and they may use different software stacks or protocols for communication. Making sure that these many systems can safely communicate with one another is one of the most difficult tasks. IoT devices are typically mobile or dynamically deployed in supply chain environments, meaning they may frequently join and leave the network. Secure communication with such devices necessitates scalable and adaptable security measures, particularly when they operate in multiple geographic locations or switch networks.

2. ENHANCING IOT DEVICE SECURITY IN SMART SUPPLY CHAINS

The Internet of Things (IoT) has completely changed how businesses operate their supply chains by enabling real-time tracking, predictive maintenance, inventory control, and more efficient logistics. But with this shift to digital, there is a noticeable increase in security issues. Because IoT devices are commonly distributed over large, networked networks, collecting, transmitting, and processing sensitive data, they are appealing targets for attacks. A smart supply chain's numerous IoT devices, sensors, and platforms must be secure in order for the data to remain confidential and for the chain to remain intact. Smart supply chains cannot function without IoT devices, which range from sensors and RFID tags to connected machinery and driverless cars. These gadgets collect information, keep an eye on procedures, and promote network connectivity.

Many IoT devices are designed with affordability and efficiency in mind, thus robust security features like encryption, secure boot, and access controls could be absent. This exposes them to attacks if they are not sufficiently protected. Smart supply chains often consist of a large number of devices across multiple manufacturers using different hardware, software, and communication protocols. This variation may make it challenging to implement uniform security policies and practices across all of the ecosystem's devices. Due to their low memory, processing power, and battery life, many Internet of Things devices have limited resources. Implementing traditional, computationally intensive security techniques, such as authentication or encryption, without degrading performance may be difficult. IoT devices can operate over a range of communication networks, including public Wi-Fi, proprietary industrial networks, and cellular networks. Frequently, they have internet connections. The potential attack surface increases when devices are exposed to external threats due to unreliable or insecure networks.

chain of supply Dozens or even millions of devices may be part of IoT networks. Ensuring consistent security upgrades across a large number of devices, managing device identities, and ensuring secure connectivity can be very challenging. Only authorized devices can access the network thanks to strong authentication. Pre-shared keys (PSK), mutual authentication, and public key infrastructure (PKI) are examples of secure authentication techniques that can be used to confirm device identities prior to enabling communication. Encrypting data while it's being transmitted and stored is one of the best ways to stop illegal access and data breaches. It is common practice to employ technologies such as IPsec, Datagram TLS (DTLS), and Transport Layer Security (TLS) to secure communication between central systems and Internet of Things devices.

3. LITERATURE SURVEY ANALYSIS

The Internet of Things (IoT) is radically altering conventional supply chains since technology allows for the real-time collection, analysis, and automation of data at various supply chain stages. Route optimization, product tracking, environmental monitoring, and better decision-making are all aided by GPS trackers, RFID tags, sensors, and other gadgets. Since the integration of IoT devices into supply chains introduces new vulnerabilities, security is a top priority.

In recent years, research has focused on the unique security vulnerabilities posed by IoT devices in smart supply chains, and many solutions have been proposed to mitigate these threats. This literature review looks at earlier studies on the issues and solutions related to supply chain IoT security. Different manufacturers produce IoT devices throughout supply chains, and these devices frequently differ in terms of hardware capabilities, communication standards, and security protocols. The complexity of maintaining consistent security policies across all devices is increased by this variability. Many IoT devices, particularly those utilized in supply chains, have limitations with regard to memory, processing speed, and battery life. This limitation makes it difficult to implement advanced security features like cryptography, anomaly detection, or complex authentication techniques that sometimes require more processing power.

Often used by IoT devices, wireless communication networks are susceptible to a number of threats, such as eavesdropping, man-in-the-middle attacks, and denial-of-service (DoS) attacks. Because IoT networks are decentralized and rely on public networks, there is a greater chance of data breaches and system disruptions. IoT devices provide a great deal of sensitive and private data, including production schedules, inventory levels, and shipment information. Protecting the confidentiality and integrity of sensitive data is essential since breaches can lead to financial losses, reputational damage, and even legal issues. The absence of generally accepted security standards makes it difficult for organizations to deploy comprehensive security protections for IoT devices in supply chains. Managing security across several systems can be difficult since various manufacturers may employ different standards.

It becomes more difficult to manage the security of an expanding number of linked devices as supply chains expand and include more IoT devices. Maintaining efficacy and efficiency while growing security systems over a large number of devices is a persistent challenge. The literature has offered a wide range of solutions to address the security concerns in supply chains driven by the Internet of Things, from organizational strategies to technology developments. Edge computing has been proposed as a way to increase security by processing data near to the IoT device rather than in a centralized cloud. Local data processing can help keep sensitive information in the supply chain ecosystem, reducing its susceptibility to external threats. Much attention has been paid to how blockchain technology might improve supply chain security, which is made possible by the Internet of Things. Blockchain technology offers an unchangeable, decentralized record that may be used to track product origins, ensure data quality, and make transaction audit trails transparent.

Techniques for machine learning (ML) and artificial intelligence (AI) can be used to detect unusual activity or potential security threats in Internet of Things networks. These technologies allow for the real-time detection of security breaches by recognizing patterns and anomalies in massive databases. Firmware and software updates on a regular basis can fix security flaws and defend against known exploits. Secure over-the-air (OTA) upgrades ensure that devices are always in the most latest security patches. Robust identity and access management (IAM) standards ensure that only authorized users and devices can access the Internet of Things network. Multi-factor authentication (MFA) and role-based access control (RBAC) are two techniques that help reduce unauthorized access. Standardizing security practices and ensuring that industry regulations (including GDPR and ISO/IEC 27001) are adhered to are essential for fostering a secure IoT environment in supply chains. Companies can get guidance on protecting IoT devices by implementing frameworks such as the Industrial Internet Consortium (IIC) security framework.

4. EXISTING APPROCHES

It is critical to secure IoT devices and their networks as they become more and more integrated into intelligent supply chains. Despite the complexity of IoT security issues in supply chains, scholars and industry professionals have created a number of strategies to deal with them. This section highlights the main strategies currently in use for improving IoT device security in intelligent supply chains, with an emphasis on the associated problems and solutions. In supply chains, where real-time data is shared among numerous stakeholders, communication security is particularly important. Ineffective communication protocols increase the likelihood of eavesdropping, man-in-the-middle attacks, and private information interception.

To ensure that data is protected at the device level and decrypted only at the designated location, many IoT devices use encryption techniques like AES and RSA. This prevents unauthorized access while data is being transmitted. Secure protocols like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are being used more and more by IoT devices in supply chains to guarantee safe data transfers over the internet. The legitimacy, secrecy, and integrity of communications between servers and Internet of Things devices are provided by these protocols. allowing Internet of Things applications, the lightweight, widely used Message Queuing Telemetry Transport (MQTT) protocol has been enhanced with secure features (such as MQTT-S) allowing encrypted communication and client authentication. Many IoT devices have minimal processing

power, which makes it challenging to apply sophisticated encryption methods. Researchers have proposed Elliptic Curve Cryptography (ECC), a lightweight cryptographic approach that provides strong security while using fewer resources.

To stop unwanted parties from altering or obtaining data, it is essential to secure access to IoT devices throughout the supply chain. A robust authentication system guarantees that the Internet of Things network may only be accessed by authorized users or devices. A lot of systems use multi-factor authentication, which enhances security by requiring devices or users to verify their identity using at least two different factors (passwords and biometric data, for example). RBAC is frequently used to specify user rights according to their function in the supply chain. For instance, only authorized staff can change inventory levels or access shipment data. This method authenticates devices and avoids spoofing by using distinctive device features, like hardware IDs.

Secure protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are being used more and more by IoT devices in supply chains to ensure secure data transfers over the internet.Managing many individuals and devices in a supply chain might make it difficult to enforce uniform access control regulations. In order to simplify access management, Advanced Identity and Access Management (IAM) frameworks are being used in large-scale IoT networks to automate the provisioning and revocation of device credentials. IoT-driven supply chains have an excellent opportunity to improve security because to blockchain's decentralized architecture. Blockchain improves data validity and lowers the possibility of fraud and manipulation by offering an unchangeable and transparent record. A product's whole supply chain lifecycle, from manufacturing to delivery, can be tracked with blockchain. A blockchain records each transaction, creating a safe and transparent audit trail. Smart contracts enable predefined actions to be automatically carried out when certain conditions are satisfied, such as payment being delivered upon successful delivery. Because these contracts are impenetrable, supply chain operations are guaranteed to remain intact.

Edge computing, for instance, processes data locally at the source, rather than sending it all to centralized cloud servers, at the IoT device or adjacent edge devices. This method decreases latency, maximizes security, and enhances real-time decision-making by retaining sensitive data on local networks. IoT devices manage data at the edge, which lowers the danger of eavesdropping and the attack surface, thereby lowering the volume of data sent to the cloud. Edge computing makes it possible to analyze data streams in real time in order to identify irregularities and possible security risks. It is possible to lessen security risks before they worsen by identifying them locally. By installing their own security features, such as firewalls or intrusion detection systems (IDS), edge devices can offer an extra layer of protection without depending on centralized systems. It could be challenging to apply sophisticated security protocols or retain massive amounts of security-related data on edge devices due to their constrained processing and storage capabilities.

5. PROPOSED METHOD

Owing to the automation, inventory tracking, and real-time data collection that IoT (Internet of Things) devices provide, modern smart supply chains rely significantly on them. In these contexts, however, the increasing usage of IoT devices poses significant security risks, such as the potential for data breaches, illicit access, and supply chain disruptions. The suggested solution aims to improve the security of IoT devices in intelligent supply chains by tackling these issues. In order to prevent physical breaches and securely store cryptographic keys, Internet of Things devices should include secure hardware components like Hardware Security Modules (HSM) or Trusted Platform Modules (TPM).

Make sure that only approved firmware is put onto devices by enforcing firmware signature and verification procedures. To identify attempts at tampering, implement automatic integrity checking during boot-up. Devices connected to the network should be required to use multi-factor authentication. In addition to conventional passwords, this also covers techniques like hardware tokens, biometrics, and device certifications. Enable secure device authentication and encrypted communication between backend systems, the cloud, and Internet of Things devices by utilizing PKI. Use contemporary encryption technologies (such as TLS 1.3 and AES-256) to transmit data securely. When processing and analyzing sensitive data in cloud-based or edge contexts, use data masking or anonymization techniques to keep it safe.

Regularly assess the security of IoT devices with AI-powered monitoring tools. Use machine learning algorithms to spot deviations from normal operational patterns, including strange data flow or connections with untrusted IP addresses. Integrate IDS to detect and manage possible security risks, such malware infestations or illegal access. Use a secure over-the-air (OTA) update method to guarantee that all Internet of Things (IoT) devices get security patches and software updates on time. Keep an eye on the device's lifespan from production to deployment to decommissioning, and ensure that security procedures are updated at every stage. Use network segmentation to isolate IoT devices from critical data systems and supply chain infrastructure. This limits the impact of any breaches to specific supply chain segments.

Ensuring the secure transport of data between IoT devices and central systems requires the use of secure communication protocols, such as MQTT with TLS and CoAP with DTLS. Utilize blockchain technology to preserve unchangeable, transparent records of data, transactions, and events across the supply chain. It ensures that no information from IoT devices, such as sensor data or inventory movements, may be altered or

manipulated. Automate security procedures with smart contracts, such as verifying device authentication or initiating security procedures in reaction to irregularities.

6. RESULT

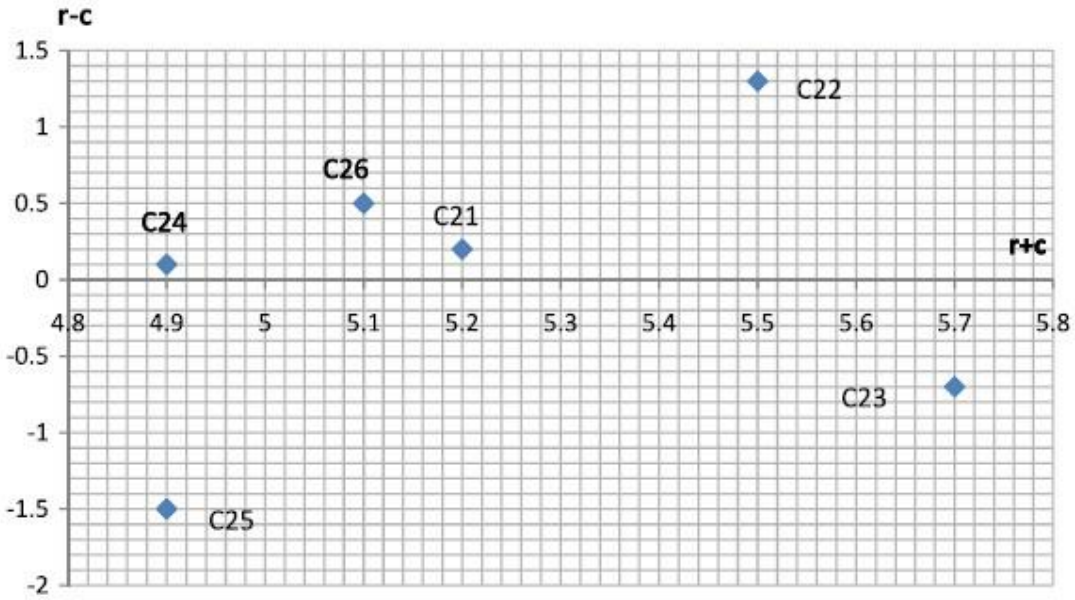

Fig. 12. The cause and effect for sub-criteria of service.

The dependability (C1) and privacy (C4) criteria are the fundamental security criteria that influence other security criteria because, as Fig. 12 illustrates, they have positive (r – c) values. The criteria of service (C2) and network (C3) are also impacted by other aspects. For the privacy criterion (C4) and the network criterion (C3), the highest values of (r + c) are discovered. The primary requirements for security components are as follows.

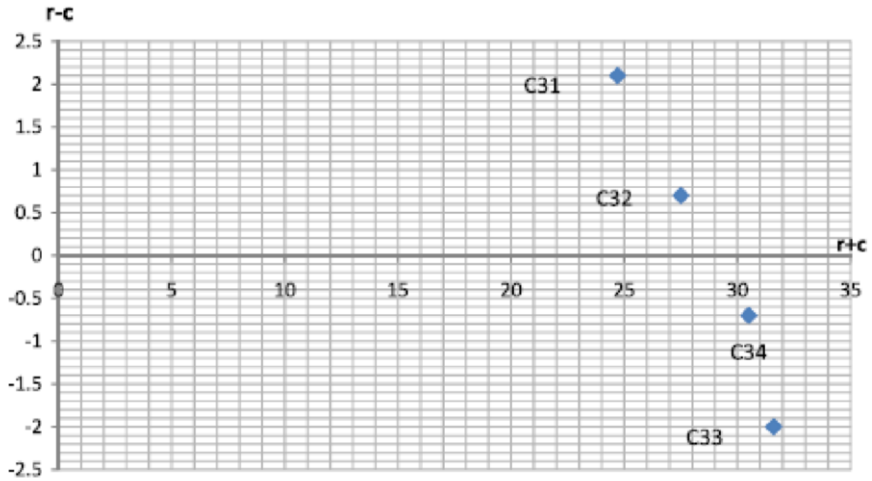

Fig. 13. The cause and effect for sub-criteria of network.

The final form of comparing service-related sub-criteria is displayed in Fig 15.

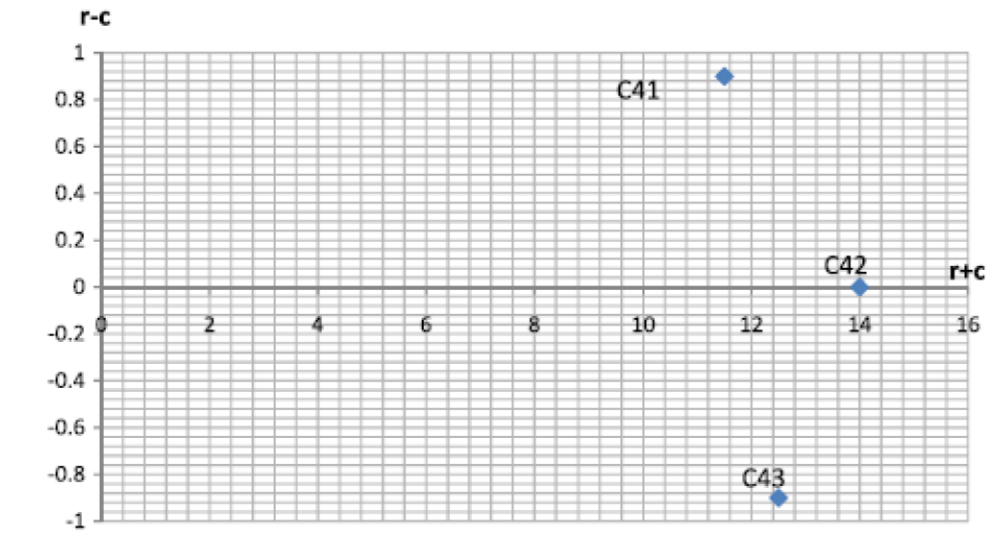

Fig. 14. The cause and effect for sub-criteria of privacy.

The final version of the comparison matrix between the criterion and the aim is displayed Fig 13. We checked the preceding matrix's consistency using the Super Decisions program. The appropriate ratio is when the consistency ratio (CR) is 0.08 < 0.1. We request that experts solely concentrate on the crucial sub-criteria that have been identified through data analysis using the neutrosophic DEMATEL approach.

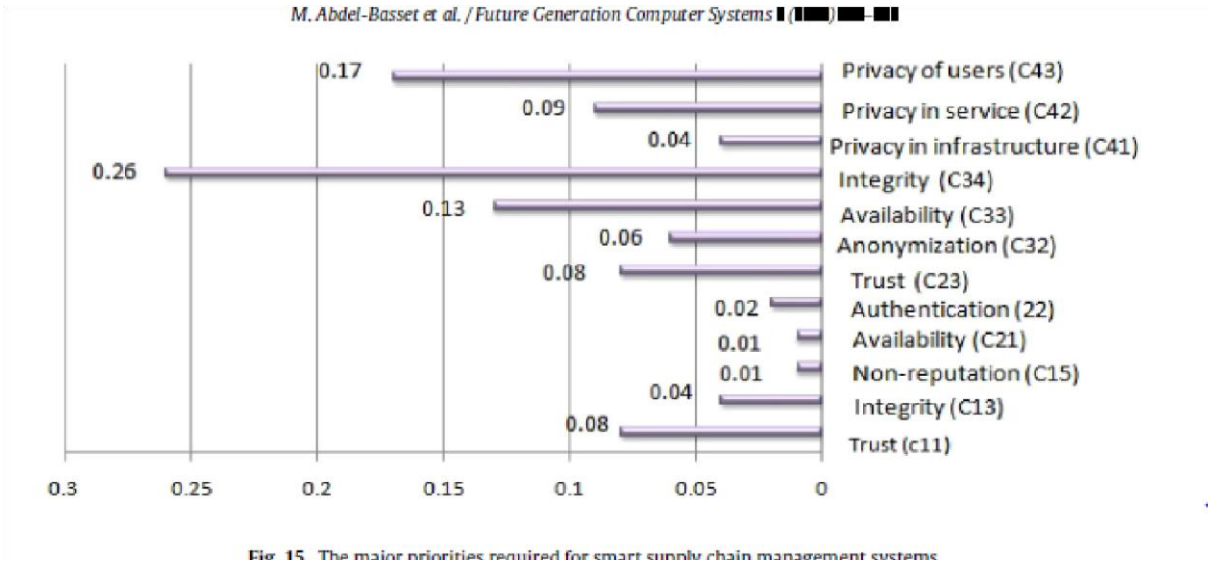

Fig. 15. The major priorities required for smart supply chain management systems.

We checked the preceding matrix's consistency using the Super Decisions program. The consistency ratio (CR) is deemed satisfactory if it falls between 0.0 and 0.1. The clear comparison matrix between the privacy-related sub-criteria is displayed.

7. CONCLUSION

Improving IoT device security in smart supply chains is essential for protecting private information, guaranteeing business continuity, and upholding confidence throughout the supply chain ecosystem. Security issues like inadequate authentication, data privacy threats, and weaknesses in legacy systems need to be addressed proactively as IoT devices are incorporated more and more into supply chain activities. The suggested solutions provide a thorough approach to addressing these issues, and they include security by design, multi-factor authentication, end-to-end encryption, blockchain for data integrity, network segmentation, and real-time anomaly detection. Businesses can protect their infrastructure from malicious actors, data breaches, and disruptions by securing IoT devices using secure communication protocols, continuous monitoring, and robust authentication processes. By implementing device lifecycle management and automated security upgrades, companies will be able to securely scale their IoT networks in response to shifting demands and new threats.

REFERENCES

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.
[2] Hui, J., & Zeng, Y. (2016). A secure IoT device authentication scheme for smart supply chains. Proceedings of the 8th International Conference on Communication Software and Networks.
[3] Roman, R., Zhou, J., & Lopez, J. (2013). On the security of modern web applications for IoT. International Journal of Computer Science and Information Security, 11(4), 43-50.
[4] Zhang, L., Li, S., & Jin, Y. (2019). Blockchain-based supply chain management: A survey. International Journal of Computer Science Issues, 16(4), 35-45.
[5] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing: A platform for internet of things and analytics. Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing.
[6] Xia, Q., Wang, S., & Zhang, Y. (2021). Blockchain-based IoT security: A survey and research directions. Journal of Network and Computer Applications, 171, 102792.
[7] Sicari, S., Rizzardi, A., & Grieco, L. A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 1-30.
[8] Zhao, J., & Zhou, W. (2018). Survey on IoT security: Vulnerabilities, threats, and countermeasures. Proceedings of the 2018 International Conference on Cyberworlds.
[9] Lu, W., Zhang, Y., & Wu, Y. (2021). A comprehensive survey on IoT security. International Journal of Computer Applications in Technology, 65(4), 364-378.
[10] Hussain, M., & Guizani, M. (2019). Internet of Things security and privacy issues. IEEE Access, 7, 115524-115537.
[11] Sheng, Q. Z., Li, J., & Lyu, M. R. (2017). Securing IoT data in supply chain management systems. IEEE Access, 5, 4550-4558.
[12] Lin, X., & Yu, L. (2020). Design of a secure IoT device in a supply chain for data privacy and integrity. IEEE Transactions on Industrial Informatics, 16(7), 4412-4421.
[13] Choi, J., & Kim, H. (2019). IoT security and privacy issues and challenges: A survey. Journal of Communications and Networks, 21(3), 271-281.
[14] Rao, G., & Sahoo, B. (2021). Blockchain-based data security and integrity model for IoTenabled supply chains. Journal of Ambient Intelligence and Humanized Computing, 12(4), 33293341.
[15] Alam, M. S., & Roy, A. (2019). Secure authentication scheme for IoT devices in the smart supply chain. Procedia Computer Science, 155, 153-160.
[16] Kumar, N., & Lin, Y. (2020). Securing smart supply chains with IoT: A review of security mechanisms and their challenges. Future Generation Computer Systems, 110, 468-483.
[17] Wang, F., & Zhang, D. (2020). A survey of security challenges in IoT-based smart supply chain management. Computers, Materials & Continua, 64(1), 11-24.
[18] Li, H., & Liu, H. (2018). Secure IoT communication protocols for supply chain applications. IEEE Internet of Things Journal, 5(6), 5105-5114.
[19] Xia, F., Yang, L. T., & Wang, L. (2018). Security and privacy for the Internet of Things: Challenges and solutions. IEEE Wireless Communications, 25(1), 12-18.
[20] Zhao, X., & Zhang, X. (2021). Lightweight encryption scheme for secure communication in IoT-enabled supply chains. Proceedings of the International Conference on Cyber Security and Cloud Computing.
[21] Gubbi, J., Buyya, R., & Marusic, S. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.
[22] Barker, S., & Morrow, M. (2017). Secure communication protocols for IoT in supply chain management. Proceedings of the International Conference on Wireless Communications and Signal Processing.
[23] Karami, S., & Zamboni, M. (2019). Securing the IoT in smart supply chains: A critical review. Security and Privacy, 2(5), e1010.
[24] Nguyen, Q., & Miao, C. (2020). A secure IoT device lifecycle management system for supply chains. IEEE Access, 8, 117857-117868.
[25] Feng, C., & Li, Y. (2019). IoT security for supply chain and smart cities. Proceedings of the International Conference on Computing, Networking, and Communications.
[26] Hassija, V., & Jha, R. (2019). Survey of IoT security frameworks: A solution for smart supply chains. Journal of Network and Computer Applications, 141, 64-75.
[27] Zhang, Y., & Wang, T. (2021). A survey on blockchain for IoT security in supply chain management. IEEE Access, 9, 112982-113004.
[28] Wang, Y., & Li, Z. (2021). Enhancing the security of IoT-enabled supply chains with multilayer defense mechanisms. Journal of Cloud Computing: Advances, Systems and Applications, 10(1), 67-80.
[29] Singh, R., & Bansal, R. (2020). IoT device security challenges in supply chain management: A survey. International Journal of Advanced Computer Science and Applications, 11(9), 521-530.
[30] Chen, W., & Jiang, Y. (2021). Blockchain-based security framework for IoT-enabled supply chains: A survey and future directions. Computers & Security, 100, 102085.