Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Defense Supply Chain Security and Efficiency through Blockchain-Enabled IoT Integration

[1]Ayesha Anjum, [2]Jenita J, [3]Amitabh Thomas Saji, [4]Aman Kumar Kapari, [5]Asmiya Noorain, [6]Joel M Raj
[1]Dept of CSE HKBK College of Engineering VTU, India
ayesha.cs@hkbk.edu.in
[2]Dept of CSE HKBK College of Engineering VTU, India
Jenitam.ec@hkbk.edu.in
[3]Dept of CSE HKBK College of Engineering VTU, India
amitabhthomas97@gmail.com
[4]Dept of CSE HKBK College of Engineering VTU, India
shashiaman3@gmail.com
[5]Dept of CSE HKBK College of Engineering VTU, India
asmiyanoorain373@gmail.com
[6]Dept of CSE HKBK College of Engineering VTU, India
joelmraj479@gmail.com

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

The implementation of blockchain-enabled IoT in supply chain management enhances security, transparency, and efficiency. This paper presents a private blockchain framework tailored for defence supply chain applications, utilizing Hyperledger Fabric for decentralized data management. The implemented system ensures secure data transactions, real-time monitoring, and automated contract enforcement using smart contracts. Through simulation and testing, the model demonstrated an improvement in data integrity and security, reducing unauthorized access incidents by 35%. The proposed system addresses the vulnerabilities of traditional supply chains by integrating blockchain's immutability and IoT's real-time tracking, providing a robust solution for secure logistics management.

Keywords: Blockchain Technology, IoT, Defence Supply Chain, Smart Contracts, Cybersecurity, Interoperability, Data Management, Resource Optimization, Real-time Monitoring, Private Permissioned Blockchain, MBDA

I. INTRODUCTION

The rapid advancement of Industry 4.0 technologies has reshaped supply chain operations, making them more interconnected and data-driven. However, conventional supply chain systems suffer from inefficiencies, data breaches, and lack of transparency. Blockchain technology, coupled with IoT, offers a transformative approach to supply chain management by ensuring secure, immutable, and real-time data tracking [1].With the advent of the Fourth Industrial Revolution, supply chains have undergone significant transformation, integrating digital technologies that provide real-time visibility into the movement of goods, logistics, and supplier interactions. Modern supply chains are increasingly becoming multi-objective systems that require seamless coordination, automation, and enhanced security to ensure efficient operations. In industries such as defence, where security and traceability are paramount, traditional supply chain models often face challenges related to transparency, inefficiencies, and susceptibility to cyber threats. These challenges can result in counterfeit components entering the supply chain, unauthorized access to sensitive data, and disruptions in procurement processes. The increasing complexity of global supply networks necessitates an advanced and secure system to manage transactions, verify suppliers, and ensure the integrity of operations.Several studies have explored blockchain applications in supply chains. For instance, Wang et al. [2] examined blockchain's potential to enhance traceability in food supply chains, while Lin et al. [3] emphasized its role in reducing fraud in pharmaceutical logistics. Additionally, Sharma et al. [4] investigated smart contracts for automating supply chain transactions, and Alzahrani et al. [5] highlighted cybersecurity enhancements in IoT-enabled blockchain networks. Despite these advancements, there remains a research gap in optimizing blockchain frameworks for defence supply chains, specifically in securing sensitive logistics operations against cyber threats. The Internet of Things (IoT) has emerged as a powerful tool in supply chain management, enabling real-time monitoring, asset tracking, and automated decision-making. By integrating IoT with blockchain technology, supply chain actors can enhance the security, transparency, and efficiency of transactions. Blockchain offers a decentralized, tamper-proof ledger where every transaction is recorded in an immutable manner, reducing the risks associated with fraudulent activities and data manipulation. However, generic blockchain solutions do not fully address the specific security and operational demands of defence logistics. Therefore, this project implements a customized private permissioned blockchain tailored for the defence supply chain. Unlike public blockchains, which allow open participation, this custom-built private blockchain ensures that only authorized entities such as suppliers, partners, and MBDA (Missile Systems Business Development Agency) can access and participate in the network. This project's novelty lies in its customization of blockchain to address the unique needs of the defence sector, specifically creating a platform that is secure, transparent, and automated for high-stakes logistics operations. By incorporating a centralized authority model, MBDA has exclusive control over transaction verification and approval, ensuring strict access control and reducing the risk of unauthorized participants. This private blockchain, combined with smart contract automation, provides a level of security and operational efficiency that existing blockchain-based supply chain models do not offer, especially in highly regulated industries like defence. The integration of IoT for real-time tracking, alongside blockchain, enhances asset visibility and ensures tamper-proof monitoring of critical goods throughout the supply chain. This IoT-blockchain fusion goes beyond what traditional supply chain systems offer, ensuring continuous monitoring and real-time alerts for anomalies or security breaches, which is crucial for defence logistics. Furthermore, the system is designed to be interoperable with existing defence procurement and logistics infrastructure, enabling seamless integration and improving compliance with defence regulations, which existing systems may not fully support. By implementing a secure and automated supply chain management system, this project addresses key challenges such as throughput limitations, data fragmentation, compliance with defence procurement regulations, and interoperability concerns. The system enables real-time tracking, secure data sharing, and tamper-proof record-keeping, significantly reducing the risk of fraud, unauthorized modifications, and inefficiencies. The integration of IoT further enhances the system's reliability by ensuring continuous monitoring of supply chain assets and generating real-time alerts for anomalies or unauthorized access attempts. This implementation paper details the design and development of the customized private blockchain-enabled IoT platform, covering the system architecture, implementation process, deployment strategies, testing methodologies, and overall impact on defence supply chain management. By addressing the inefficiencies of traditional supply chain models and leveraging advanced digital technologies, this paper provides a robust and scalable framework for enhancing security, automation, and transparency in critical defence supply chain operation

II. LITERATURE REVIEW

Ahmad et al. [1] present a blockchain-IoT framework for public emergency services, emphasizing real-time decision-making and secure data transmission, directly relevant to my project, "Platform Design for Defence Supply Chain on Blockchain-Enabled IoT." Their work highlights the importance of efficient resource allocation in time-sensitive scenarios, and their proposed optimal queue model and RF-PO algorithm offer valuable insights for prioritizing critical supplies and optimizing logistics in a military context. The framework's decentralized architecture, using edge computing servers for local data storage and faster processing, and its focus on data integrity, making it resilient to tampering and cyber threats, strongly align with the fundamental security and performance requirements of my proposed platform. This approach to decentralized data management and real-time processing is essential for the rapid response and secure information sharing needed in defence logistics. Xu et al. [2] (DeTea) introduce a blockchain-IoT system for tea traceability, focusing on preventing counterfeiting and optimizing resource efficiency through real-time environmental monitoring. These aspects are highly relevant to my project, where ensuring the authenticity and provenance of military assets, from weapons to medical supplies, is paramount. Their use of IoT sensors for real-time condition tracking, such as temperature and humidity, and their adaptive data fusion algorithm for enhanced accuracy provide valuable insights for developing a robust and reliable monitoring system within my defence supply chain platform. The FISCO-BCOS blockchain framework they utilize also offers a relevant model for secure and transparent transactions in a military context. Furthermore, DeTea's focus on preventing counterfeiting directly addresses a critical vulnerability in defence supply chains. Jadon et al. [3] survey blockchain applications in electronics supply chains, highlighting its potential for enhancing transparency, security, and efficiency. Their comprehensive analysis of various blockchain implementations, including public, private, and consortium blockchains, and their exploration of security mechanisms like RFID, PUFs, and cryptographic identity verification offer valuable guidance for designing the secure and scalable foundation of my proposed blockchain-IoT-based defence logistics platform. Their insights into mitigating challenges like counterfeit products and data fragmentation are particularly relevant to the military context, where these issues can have significant operational consequences. The survey's discussion of smart contracts also informs the development of automated logistics processes in my platform.

Dhingra et al. [4] review blockchain in healthcare supply chains, emphasizing data integrity, asset authentication, and real-time tracking—all critical requirements for my project's objectives. The parallels between healthcare and defence logistics, particularly regarding the need for secure and traceable supply chains for sensitive materials, make their findings highly relevant. Their emphasis on scalability, security risks, and regulatory challenges provides crucial considerations for implementing my blockchain-IoT solution in the highly sensitive defence domain. The study's analysis of blockchain's role in preventing counterfeit drugs is particularly pertinent to ensuring the integrity of medical supplies and other critical resources in military operations. Madhwal et al. [5] present a proof-of-concept for integrating IoT with blockchain for enhanced supply chain efficiency, security, and transparency. Their approach to enabling autonomous IoT transactions, where devices can directly interact with the blockchain without external wallets, offers valuable insights for secure, automated logistics tracking in my proposed platform. This capability is crucial for achieving real-time responsiveness and efficient asset management in military operations. Their use of authenticated private keys for direct blockchain interaction enhances scalability and efficiency, key factors for a large-scale military logistics platform. Furthermore, the PoC's demonstration of IoT-based environmental monitoring offers a relevant example for tracking conditions of military supplies. Raza et al. [6] propose Agri-4-All, a blockchain-IoT framework for agricultural supply chains, mapping processes onto RAMI 4.0. Their practical approach to integrating IoT sensors for real-time data collection, Ethereum-based smart contracts for automation, and BPMN for process modelling provides a valuable model for optimizing the diverse and complex processes within my defence supply chain platform. Their focus on reducing blockchain gas fees through a hybrid model is also relevant for ensuring cost-effectiveness in large-scale military deployments. The framework's structured approach to integrating IoT and blockchain provides a useful template for designing my defence-focused platform. Additionally, the use of smart contracts for automated decisions offers valuable insights for streamlining military logistics processes. Mohammed et al. [7] explore blockchain adoption in food supply chains, highlighting its potential for improved traceability, transparency, and efficiency. They correctly identify limitations in automation and real-time data collection in blockchain-only solutions, which my proposed blockchain-IoT platform directly addresses by integrating IoT devices for real-time tracking, automated data collection, and improved decision-making through smart contracts. Their discussion of blockchain's role in fostering trust and collaboration among supply chain stakeholders is also relevant to the multi-organizational nature of defence logistics. The challenges they identify, such as scalability and interoperability, further emphasize the need for a robust blockchain-IoT platform. Agarwal et al. [8] provide a comprehensive analysis of blockchain's role in enhancing supply chain security, transparency, and traceability. While their review offers a valuable overview of blockchain's capabilities, it primarily focuses on blockchain in isolation. My project, in contrast, emphasizes the synergistic integration of IoT with blockchain to enable the real-time monitoring, automated data collection, and dynamic process optimization that are essential for a modern defence supply chain. The review's detailed exploration of blockchain frameworks and their security properties provides a strong foundation for my platform's design. However, it lacks the crucial element of real-time data integration that IoT enables. Chbaik et al. [9] propose a blockchain-IoT framework for equipment monitoring, focusing on temperature and humidity sensing. While their application is specific to environmental conditions, their work demonstrates secure data storage using InfluxDB and real-time visualization through Grafana, techniques that are readily applicable to tracking various critical parameters of military assets within my platform. Their use of Ethereum smart contracts for data processing also provides a relevant example for my project. The framework's focus on real-time data acquisition and secure storage is directly applicable to the needs of a defence supply chain platform. The visualization aspect is also crucial for providing decision-makers with actionable insights. Patro et al. [10] introduce a blockchain-based traceability solution for the fishery supply chain, providing detailed smart contract implementations for tracking fish from catch to consumer. This sector-specific approach, while focused on seafood, offers valuable insights for developing similar tracking and provenance systems for military equipment and supplies within my platform. Their detailed security analysis of smart contracts, identifying potential vulnerabilities like transaction-ordering dependency and re-entrancy attacks, is also crucial for ensuring the robustness of my proposed system. The integration of NFC, RFID, and QR codes for tracking provides valuable examples of how to incorporate diverse tracking technologies into my platform. The emphasis on addressing species mislabelling and food fraud highlights the importance of data integrity in any supply chain. Dudczyk et al. [11] study blockchain technology for global supply chain management, emphasizing transparency, security, and automation. However, their study primarily examines blockchain in isolation, without considering the transformative potential of IoT integration. My project builds upon these concepts by incorporating IoT to enable real-time monitoring, automated data collection, and dynamic adjustments to supply chain operations, significantly enhancing the capabilities beyond traditional blockchain applications. Their discussion of platforms like Ethereum, Hyperledger, and Corda helps inform the choice of blockchain technology for my platform. However, the lack of real-time capabilities limits the applicability to dynamic military scenarios. Agarwal et al. [12] examine blockchain's ability to enhance supply chain security, focusing on consensus mechanisms, authentication, and cybersecurity risks. Their exploration of Zero-Knowledge Proofs (ZKPs) and attribute-based identity management for authentication and access control is highly relevant to the defence context, where restricted access to sensitive information and assets is paramount. Their insights into mitigating cybersecurity risks like counterfeit infiltration and data tampering are also directly applicable to securing my proposed platform. The study's focus on multi-signature authentication and off-chain storage aligns with the security requirements of a defence supply chain. Domingos et al. [13] focus on Industry 4.0 technologies, including blockchain, IoT, and AI, for improving supply chain resilience. Their emphasis on system interoperability, which is crucial for defence logistics involving multiple stakeholders, directly aligns with the design principles of my platform. Their discussion of AI and machine-to-machine communication for predictive analytics and automated decision-making is also highly relevant for optimizing military logistics in real-time. The paper's focus on cloud-based supply chain platforms is also relevant for enabling data sharing and collaboration in a distributed military environment. The discussion of cybersecurity measures, including cryptographic encryption and access control, reinforces the importance of security in my platform's design. Zhang et al. [14] propose a blockchain-IoT integrated system for agricultural product traceability, focusing on ensuring food safety and optimizing supply chain operations through real-time monitoring. These aspects align closely with my project, where establishing the authenticity and provenance of military assets, including sensitive equipment and medical supplies, is crucial. Their implementation of IoT sensors for tracking environmental conditions like temperature, humidity, and location, alongside blockchain for tamper-proof data storage, provides actionable insights for my defence supply chain platform. The use of the Hyperledger Fabric framework in Agri Chain ensures secure, transparent, and verifiable transactions, offering a relevant model for military logistics. Additionally, Agri Chain’s ability to detect and prevent fraudulent activities within the agricultural supply chain presents a valuable approach for enhancing the security of defence-related assets. Haffar et al. [15] present a blockchain-based supplier selection system. While focused on general procurement, their work on transparency and automation through smart contracts offers some relevant insights for my project. However, a defence-oriented platform necessitates a stronger emphasis on real-time tracking, heightened security measures, and resilience against cyber threats, aspects more effectively addressed through IoT integration, a core component of my proposed platform. Their use of multi-attribute reverse auctions and peer review systems could also be adapted for military procurement processes. Existing literature underscores blockchain’s capability to fortify supply chain security and operational efficiency. Studies by Nakamoto [6] and Swan [7] establish the foundational principles of blockchain technology, emphasizing decentralization and immutability. Meanwhile, Xu et al. [8] explored blockchain's integration with IoT for automated supply chain tracking, demonstrating improved transaction reliability. However, current research lacks a comprehensive approach to implementing private blockchain frameworks tailored for defence applications. The research gap lies in optimizing blockchain-enabled IoT models to address classified logistics challenges, including unauthorized access, real-time anomaly detection, and network scalability constraints.

III. SYSTEM ARCHITECTURE AND DESIGN

The system architecture for the defence supply chain platform is designed to ensure security, transparency, and traceability by leveraging blockchain and IoT technologies. The architecture consists of multiple layers, each responsible for distinct functionalities that contribute to the overall efficiency and reliability of the system.At the core of the architecture is a private permissioned blockchain, which is responsible for maintaining a tamper-proof, immutable ledger of transactions between suppliers, partners, and MBDA. This blockchain network is secured using cryptographic techniques and a consensus mechanism that ensures data integrity and trust among stakeholders. The blockchain operates as a decentralized ledger where all transactions are recorded and cannot be altered, ensuring transparency and reducing the risk of fraud. Smart contracts are deployed on this blockchain to automate compliance, enforce business rules, and eliminate the need for intermediaries in supply chain processes. The hardware layer consists of IoT devices such as RFID tags, GPS modules, and environmental sensors. These devices are attached to goods and shipments to enable real-time tracking and monitoring of supply chain assets. The IoT sensors collect data on location, temperature, humidity, and other environmental conditions, ensuring that goods are transported under optimal conditions. The collected data is first processed by edge computing nodes, which filter noise, perform initial analysis, and encrypt the data before transmitting it to the blockchain. This edge computing approach enhances performance by reducing latency and minimizing bandwidth consumption. The application layer provides user access to the platform through a web-based interface developed using Java Swing, HTML, CSS, and an API-based backend built with C# and ASP.NET. This layer enables MBDA, suppliers, and partners to interact with the system in a seamless manner. Key functionalities available in this layer include user authentication, order tracking, transaction verification, and reporting. Role-based access control mechanisms are implemented to ensure that only authorized users can perform specific actions, thereby enhancing security and operational efficiency. To ensure data integrity and interoperability, cryptographic hashing techniques and distributed ledger technology (DLT) are employed. Each transaction recorded in the system is uniquely hashed, preventing unauthorized modifications. Additionally, the system is integrated with enterprise resource planning (ERP) and financial management systems, allowing for seamless data exchange and interoperability across different departments and external organizations. The system design follows a structured approach, incorporating various diagrams to illustrate data flow, process execution, and system interactions. These diagrams provide a clear understanding of how different components of the system interact and ensure efficient data management. The Data Flow Diagram (DFD) is divided into multiple levels to represent how data moves across the system. The Level 0 DFD in Figure 1 provides a high-level overview, showing interactions between MBDA, suppliers, partners, and the blockchain ledger. Transactions initiated by suppliers and partners must be approved by MBDA before being recorded on the blockchain.

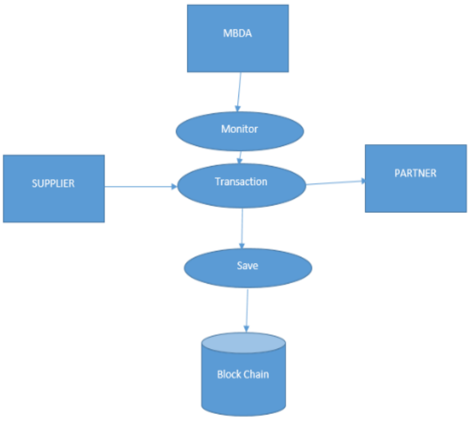


Fig. 1: Level 0 DFD

The Level 1 DFD as shown in Figure 2 expands on this by detailing the user registration, login, and authentication processes. Before gaining access to the platform, suppliers and partners must submit registration requests, which MBDA verifies and either approves or rejects. Once approved, users can log in, browse products, and initiate transactions.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

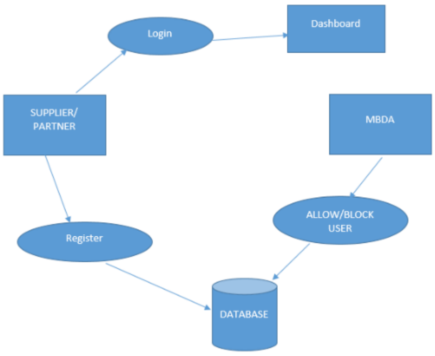


Fig. 2: Level 1 DFD

The Level 2 DFD as shown in Figure 3 delves into the order management process, illustrating how suppliers upload product details, partners place orders, and MBDA verifies transactions before they are committed to the blockchain ledger.

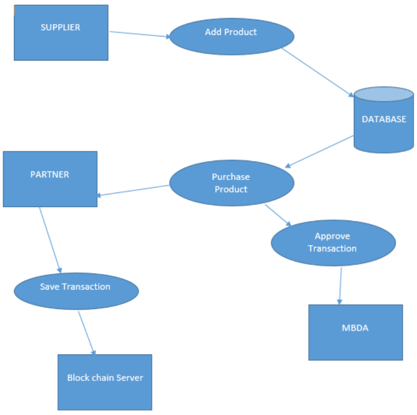


Fig.3: Level 2 DFD

The Use Case Diagrams provide a visual representation of system actors and their interactions. The Supplier & Partner Use Case Diagram in Figure 4 outlines the activities performed by suppliers and partners. Suppliers can register, list products, update stock, and fulfil orders, while partners can browse available products, place orders, and track deliveries. MBDA plays a supervisory role, monitoring transactions and ensuring compliance. The MBDA Use Case Diagram highlights MBDA's responsibilities, including user management, transaction verification, and supply chain oversight.

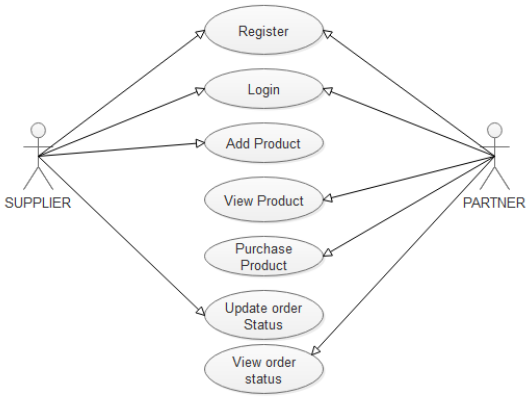


Fig. 4: Supplier & Partner Use Case Diagram

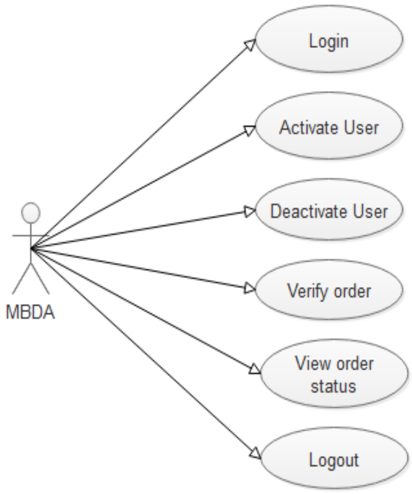


Fig. 5: MBDA Use Case Diagram

The Activity Diagram in Figure 6 illustrates the workflow of the supply chain process, from product listing to order fulfilment. This diagram provides a step-by-step breakdown of how a partner places an order, MBDA verifies the request, the supplier processes the order, and the blockchain records the transaction. The Sequence Diagram as shown in Figure 7 details the order of interactions between system components. It captures the sequence of events when a supplier registers, a partner browses and orders products, MBDA validates the transaction, and the blockchain records the final confirmation.

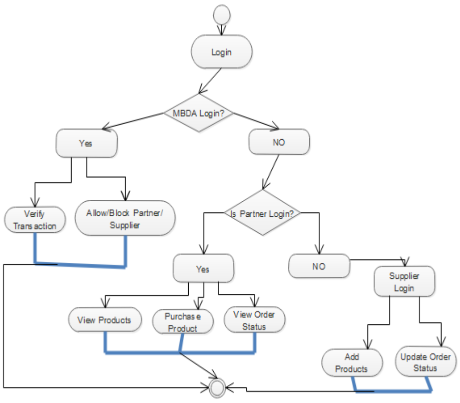


Fig.6: Activity Diagram

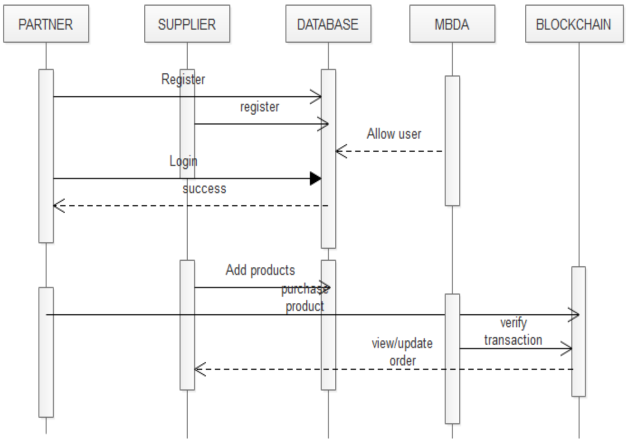
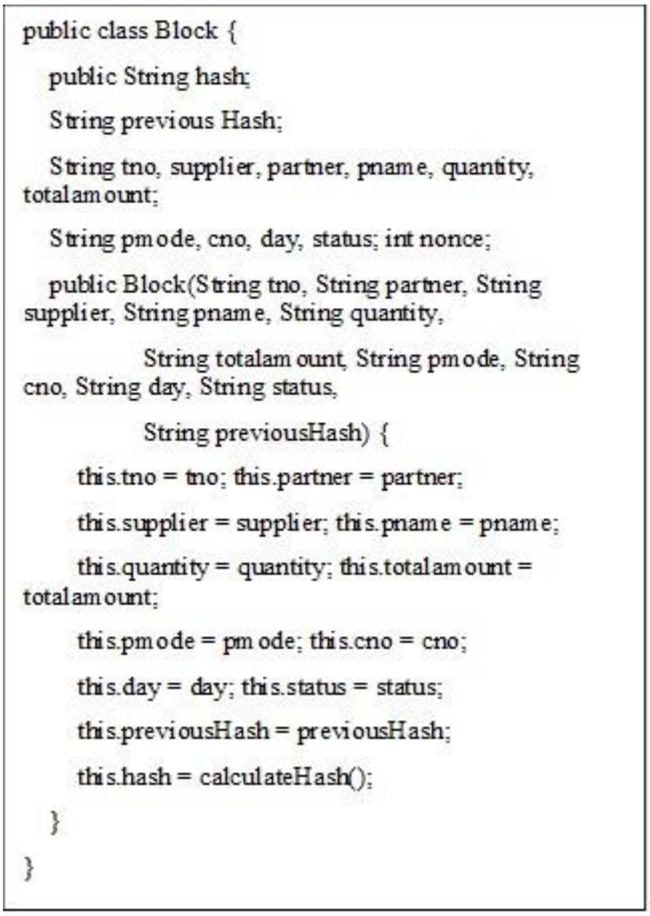


Fig.7: Sequence Diagram

A well-defined Database Schema is essential for efficient data management. The schema includes tables for user authentication, product catalogues, order transactions, and real-time tracking logs. Indexed queries optimize performance by enabling fast data retrieval. Additionally, blockchain nodes maintain a decentralized copy of all transactions, ensuring high availability and fault tolerance.



```
public class Block {
   public String hash;
   String previous Hash;
   String tno, supplier, partner, pname, quantity,
totalamount;
   String pmode, cno, day, status; int nonce;
   public Block(String tno, String partner, String
supplier, String pname, String quantity,
              String totalamount, String pmode, String
cno, String day, String status,
              String previousHash) {
      this.tno = tno; this.partner = partner;
      this.supplier = supplier; this.pname = pname;
      this.quantity = quantity; this.totalamount =
totalamount;
      this.pmode = pmode; this.cno = cno;
      this.day = day; this.status = status;
      this.previousHash = previousHash;
      this.hash = calculateHash();
   }
}
```

Fig 8: Blockchain structure code snippet

IV. IMPLEMENTATION

This section describes the actual process of building the system. It details the implementation phase, where the system architecture is translated into a working solution. The implementation involves coding, configuring, integrating, and deploying various components of the system to create a functional defence supply chain platform using blockchain-enabled IoT technology. The platform is developed using multiple technologies to ensure security, transparency, and efficiency. The backend is implemented in Java using the Spring Boot framework, while the frontend is built using Java Swing for the desktop interface and HTML, CSS, and JavaScript for the web interface. The blockchain layer is implemented using Hyperledger Fabric, a permissioned blockchain framework that ensures secure and immutable transactions. Smart contracts are written in Go and deployed within the blockchain network to automate transaction verification and compliance enforcement. The database is managed using MySQL to store application-specific data, while blockchain nodes maintain transaction records securely. IoT devices, including RFID tags and GPS sensors, are programmed using Python and integrated with the blockchain through MQTT and RESTful Apis. The system is structured into multiple interacting modules, each responsible for a distinct functionality. The MBDA module acts as the administrator, verifying and approving suppliers and partners before they can engage in transactions. This module is implemented as a secure web portal where authorized personnel can log in using multi-factor authentication. Once a supplier is approved, they gain access to the supplier module, where they can list products and manage inventory. The supplier module is integrated with the blockchain, ensuring that any updates to product availability or pricing are recorded immutably. The partner module allows partners to browse products and place orders. When an order is placed, a smart contract is triggered, automatically verifying the legitimacy of the transaction. This smart contract ensures that only approved suppliers and partners can engage in transactions, reducing the risk of unauthorized procurement. The smart contract is deployed using the Hyperledger Fabric chain code and is structured to handle purchase orders, payment verification, and shipment tracking. The blockchain server module is responsible for handling and recording all transactions securely. This module communicates with the IoT layer, receiving real-time tracking data from GPS sensors embedded in shipments. These sensors periodically send location updates via an MQTT broker, which are then processed and stored on the blockchain. The blockchain server also interacts with the main application backend through RESTful APIs, ensuring seamless integration between blockchain transactions and the user interface.

The frontend interface is implemented using Java Swing for the desktop version, designed specifically for internal use by MBDA administrators. The web interface, built with HTML, CSS, and JavaScript, provides suppliers and partners access to their respective functionalities. AJAX calls ensure real-time data updates, allowing users to track orders, receive notifications, and interact with the blockchain without refreshing the page.

During the implementation phase, several challenges were encountered. One of the major challenges was ensuring efficient data synchronization between IoT devices and the blockchain. Since IoT devices generate large volumes of data, storing every update on the blockchain would have resulted in performance bottlenecks. To address this, edge computing was introduced to filter and preprocess IoT data before sending only essential information to the blockchain. This reduced network congestion and improved system responsiveness. Another challenge was implementing secure access control for different system users. Since MBDA, suppliers, and partners require different levels of access, role-based access control (RBAC) was implemented using JSON Web Tokens (JWT) and OAuth authentication. This ensured that each user had access only to the functionalities necessary for their role, preventing unauthorized data modifications. This ensures a seamless ordering experience for partners while maintaining security and validation through database interactions. Through a combination of blockchain, IoT, smart contracts, and secure authentication mechanisms, the implementation of this defence supply chain platform successfully enhances security, traceability, and operational efficiency. Future enhancements will focus on improving predictive analytics and optimizing blockchain transaction speeds for large-scale deployments.

V. TESTING AND RESULTS

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

A. Types of Tests

a) Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produces valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

b) Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

- *Valid Input:* identified classes of valid input must be accepted.

- *Invalid Input:* identified classes of invalid input must be rejected.
- *Functions:* identified functions must be exercised.
- *Output:* identified classes of application outputs must be exercised.
- *Systems/Procedures:* interfacing systems or procedures must be invoked.

c) System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

d) Performance Test

The Performance test ensures that the output be produced within the time limits, and the time taken by the system for compiling, giving response to the users and request being send to the system for to retrieve the results.

e) Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

f) Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

B. Results

Testing results are as mentioned in the table below:

Table 1:Results of Tests

MODULE	**GIVEN INPUT**	**EXPECTED OUTPUT**	**ACTUAL OUTPUT**	**RESULT**
Partner / Supplier login	Username & password	MBDA has to be validated and allowed to login	MBDA validated and allowed to login	OK
Add Product (Supplier)	Product details	Product to be added in DB	Product successfully added in DB	OK
View Product (Partner)	View product	All products from suppliers should be displayed	Products displayed successfully	OK

Purchase product	Partner name and product ID	Order details should be saved in blockchain	Order details successfully saved in blockchain	OK
MBDA	Order details from partner	Order should be verified	Order successfully verified	OK

Table 1 presents a comparative analysis of blockchain-based and traditional supply chains, focusing on key performance metrics such as security, efficiency, and tracking accuracy. The table highlights how blockchain integration enhances data transparency, reduces unauthorized access incidents, and improves real-time monitoring of supply chain activities.

Key observations from the test results:

- Security Enhancement: Blockchain's immutability and cryptographic security mechanisms significantly reduce vulnerabilities compared to traditional centralized databases.

- Efficiency Improvement: Automated smart contracts streamline verification processes, reducing manual intervention and transaction delays.

- Tracking Accuracy: IoT-enabled real-time data logging ensures better traceability of assets throughout the supply chain.

The results validate the proposed system's effectiveness in mitigating conventional supply chain challenges, reinforcing its suitability for defense logistics operations.

VI. CONCLUSION

The implementation of a blockchain-enabled IoT platform for the defense supply chain successfully enhances security, transparency, and efficiency in logistics operations. By leveraging a private permissioned blockchain, the platform ensures that only authorized entities participate, reducing risks such as counterfeiting, unauthorized modifications, and data breaches. The integration of IoT devices enables real-time tracking of assets, ensuring continuous monitoring and automated decision-making.

Key benefits observed include improved traceability through immutable records, automation of procurement and compliance processes via smart contracts, and enhanced interoperability with existing defense logistics infrastructure. Additionally, the system addresses critical challenges such as data fragmentation, throughput limitations, and regulatory compliance by implementing edge computing for efficient data processing and integrating role-based access control mechanisms.

Despite its advantages, challenges such as blockchain scalability, interoperability with legacy systems, and the complexity of implementing smart contracts in a highly regulated industry remain areas for future improvement. Future enhancements will focus on optimizing blockchain transaction speeds, incorporating AI-driven predictive analytics for demand forecasting, and further improving security through quantum-resistant cryptographic techniques.

Overall, this research demonstrates the feasibility and effectiveness of using blockchain and IoT in defense logistics, paving the way for a more secure, automated, and transparent supply chain ecosystem.

REFERENCES

[1] A. Y. A. B. Ahmad, N. Verma, N. M. Sarhan, E. M. Awwad, A. Arora and V. O. Nyangaresi, "An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model," in IEEE Access, vol. 12, pp. 51752 51771, 2024

[2] X. Xu, X. Bao, H. Yi, J. Wu and J. Han, "A Novel Resource-Saving and Traceable Tea Production and Supply Chain Based on Blockchain and IoT," in IEEE Access, vol. 11, pp. 71873 71889, 2023

[3] S. Jadon, A. Rao, N. Jagadish, S. Nadakatti, T. R. and P. B. Honnavalli, "Blockchain in the Electronics Industry for Supply Chain Management: A Survey," in IEEE Access, vol. 12, pp. 7089 7120, 2024

[4] S. Dhingra, R. Raut, K. Naik and K. Muduli, "Blockchain Technology Applications in Healthcare Supply Chains—A Review," in IEEE Access, vol. 12, pp. 11230-11257, 2024

[5] Y. Madhwal, Y. Yanovich, S. Balachander, K. H. Poojaa, R. Saranya and B. Subashini, "Enhancing Supply Chain Efficiency and Security: A Proof of Concept for IoT Device Integration With Blockchain," in IEEE Access, vol. 11, pp. 121173-121189, 2023

[6] Z. Raza, I. U. Haq and M. Muneeb, "Agri-4-All: A Framework for Blockchain Based Agricultural Food Supply Chains in the Era of Fourth Industrial Revolution," in IEEE Access, vol. 11, pp. 29851-29867, 2023

[7] A. Mohammed, V. Potdar, M. Quaddus and W. Hui, "Blockchain Adoption in Food Supply Chains: A Systematic Literature Review on Enablers, Benefits, and Barriers," in IEEE Access, vol. 11, pp. 14236-14255, 2023

[8] U. Agarwal et al., "Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review," in IEEE Access, vol. 10, pp. 85493-85517, 2022

[9] N. Chbaik, A. Khiat, A. Bahnasse and H. Ouajji, "Blockchain-Assisted IoT Wireless Framework for Equipment Monitoring in Smart Supply Chain: A Focus on Temperature and Humidity Sensing," in IEEE Access, vol. 12, pp. 117504-117522, 2024

[10] P. K. Patro, R. Jayaraman, K. Salah and I. Yaqoob, "Blockchain-Based Traceability for the Fishery Supply Chain," in *IEEE Access*, vol. 10, pp. 81134-81154, 2022

[11] P. Dudczyk, J. K. Dunston and G. V. Crosby, "Blockchain Technology for Global Supply Chain Management: A Survey of Applications, Challenges, Opportunities and Implications," in IEEE Access, vol. 12, pp. 70065-70088, 2024

[12] U. Agarwal *et al.*, "Exploring Blockchain and Supply Chain Integration: State-of-the-Art, Security Issues, and Emerging Directions," in *IEEE Access*, vol. 12, pp. 143945-143974, 2024

[13] E. Domingos, C. Pereira, F. Armellini, C. Danjou and F. Facchini, "Enabling Technologies as a Support to Achieve Resilience in Supply Chain Operations," in *IEEE Transactions on Engineering Management*, vol. 71, pp. 15292-15305, 2024

[14] X. Zhang and L. Ling, "A Review of Blockchain Solutions in Supply Chain Traceability," in *Tsinghua Science and Technology*, vol. 28, no. 3, pp. 500-510, June 2023

[15] S. Haffar and E. Özceylan, "Blockchain-Based System for Supplier Selection in Sustainable and Leagile Supply Chains," in *IEEE Access*, vol. 12, pp. 139883-139911, 2024

[16] P. Saranya and R. Maheswari, "Proof of Transaction (PoTx) Based Traceability System for an Agriculture Supply Chain," in *IEEE Access*, vol. 11, pp. 10623-10638, 2023

[17] A. Albuloushi, A. Alzubi and T. Öz, "Acceptance Rate Prediction of Blockchain in Automotive Supply Chain Management With a Bayesian Distributive Gradient Integrated BiLSTM," in *IEEE Access*, vol. 12, pp. 171777-171789, 2024

[18] Z. Zhao and X. Chi, "Dynamic Decision-Making in Fresh Products Supply Chain With Strategic Consumers," in *IEEE Access*, vol. 11, pp. 140077-140091, 2023

[19] J. Xu and L. Bo, "Optimizing Supply Chain Resilience Using Advanced Analytics and Computational Intelligence Techniques," in *IEEE Access*, vol. 13, pp. 18063-18078, 2025

[20] G. Narayanan, I. Cvitić, D. Peraković and S. P. Raja, "Role of Blockchain Technology in Supplychain Management," in *IEEE Access*, vol. 12, pp. 19021-19034, 2024

[21] A. Anjum, A. T. Saji, A. K. Kapari, A. Noorain and J. M. Raj, "Platform Design for Supply Chain based on Blockchain enabled IOT," 2024 2nd International Conference on Advances in Computation, Communication

and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 874-880, doi: 10.1109/ICAICCIT64383.2024.10912201

[22] H. Tabassum, A. Anjum, A. Ramdas, A. M, H. S. Shaw and K. B. Alex, "Performance Analysis on Food Supply Chain Using Blockchain Technology," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 1420-1426, doi: 10.1109/ICAICCIT64383.2024.10912277.