SYNOPSIS

OF

MEGA PROJECT

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

Aaditya Borkar	Ishad Pande	Sangita Borkute	Yashasvi Sherke
CSE/RN/03	CSE/RN/25	CSE/RN/53	CSE/RN/68

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GOVERNMENT COLLEGE OF ENGINEERING, NAGPUR

1. INTRODUCTION

Today’s supply chains rely entirely on digital systems to connect manufacturers, shippers, and retailers. The major security problem is that these systems often depend on a single, central point of control. This design creates a critical weakness, as a powerful cyberattack could target this central point and paralyze the entire network. The NotPetya cyberattack, for instance, demonstrated this exact danger by shutting down global logistics operations, causing chaos and massive losses simply because the system had a single point of failure. Our project, the “Supply Chain Transparency and Security Platform,” is designed specifically to prevent this kind of collapse. Using blockchain technology, we build a more resilient network by creating a shared and secure operational record that is copied and distributed among all partners. This approach removes the single point of failure. If one partner is hit by a cyberattack, the rest of the supply chain is protected and can continue to function because the vital information is not lost and remains securely accessible to everyone else.

2. LITERATURE SURVEY

Recent literature and post-incident analyses of major cyberattacks have identified a critical vulnerability in the modern supply chain: the fragility of its centralized digital infrastructure. While traditional issues like traceability remain important, the focus is shifting towards the existential threat posed by systemic cyberattacks that can halt global operations, making system resilience the paramount security concern.

Post-mortems of major cyber incidents, extensively covered by publications like *Wired* and cybersecurity firms such as Mandiant, consistently identify centralized IT systems as the core vulnerability in modern supply chains. The 2017 NotPetya attack serves as the definitive case study. Analysis revealed how the malware exploited a single entry point to propagate uncontrollably through the centralized networks of logistics giant Maersk, forcing the shutdown of ports across the globe. A 2024 report by Deloitte on digital risk management concludes that such centralized architectures create a "disproportionate concentration of risk," where a single digital breach can trigger a global, physical paralysis of assets. The literature

establishes a clear consensus: the interdependence of partners on a single, vulnerable data hub is the primary architectural flaw threatening the modern supply chain.

Reports from national cybersecurity agencies, including India's Computer Emergency Response Team (CERT-In), highlight a strategic shift in threats against critical infrastructure. The goal of sophisticated attackers is no longer merely data theft, but complete operational disruption. The 2025 IBM Security X-Force Threat Intelligence Index notes that destructive malware and ransomware designed to "incapacitate business operations" are now the leading threat to the logistics and manufacturing sectors. Research from Accenture further quantifies the impact, finding that the average downtime from a destructive attack now exceeds 21 days, with recovery costs often reaching hundreds of millions of dollars. This body of research indicates that the most significant security challenge is not just protecting data at rest, but ensuring the entire network can continue to operate even when a key participant is actively under digital siege.

3. PROBLEM STATEMENT

A critical security flaw is inherent in the architecture of modern logistical networks: their fundamental reliance on centralized data systems. This design creates a single point of failure, rendering entire ecosystems dangerously susceptible to targeted cyber warfare. An attack on this central hub, as exemplified by the NotPetya incident that devastated global supply chains, extends far beyond data compromise to instantly cripple the entire operational network. By exploiting this single vulnerability, an attacker can paralyze the core functions of tracking, shipping, and managing goods, triggering a complete system-wide collapse and shattering the digital trust that underpins partnerships across the supply chain.

4. OBJECTIVES

Our project has the following key goals:

I. To build a **secure website using blockchain** that is designed to keep the supply chain running smoothly, even during a major cyberattack.

II. To give every product a **secure digital record** on the blockchain, so its information is safe and can be tracked accurately, even if one of our partners gets hacked.

III. To use **automatic digital rules (smart contracts)** to continuously run compliance-related checks, ensuring all steps meet regulatory standards.

IV. To provide a **personalized dashboard for each member** whether a manufacturer, distributor, or retailer showing them the specific data and security alerts relevant to their role.

V. To give all **members of the supply chain** provable confidence that the system will always stay online and be secure, allowing business to continue without interruption.

5. METHODOLOGY

The development of this platform will adhere to the Waterfall model. This sequential software development lifecycle is selected to enforce a structured, phase-gated approach, ensuring that all security and architectural requirements are formally reviewed and approved before subsequent phases commence.

5.1 Requirement Gathering and Analysis

- This phase will involve a thorough analysis of post-incident reports and cybersecurity literature concerning systemic attacks, such as NotPetya, to identify common architectural vulnerabilities.
- A formal Software Requirement Specification (SRS) document will be created, detailing all functional and non-functional requirements with a primary emphasis on operational continuity, data integrity, and system resilience.
- Security requirements, including role-based access control (RBAC) policies and data encryption standards, will be formally defined and documented.

5.2 System Design

- The system architecture will be designed to be fully decentralized, thereby eliminating any single point of failure and ensuring high availability for all network

participants.

- The logic for the smart contracts will be designed to govern the immutable logging of all supply chain events and the state changes of assets on the ledger.
- High-fidelity wireframes and mockups for the user interface will be developed, detailing the personalized dashboards, data visualization components, and administrative interfaces for each stakeholder role.

5.3 Implementation

- This phase will consist of the development of the frontend client and backend services using the specified technology stack.
- Smart contracts will be coded in their respective languages (e.g., Solidity), then compiled and deployed to the target blockchain network to manage the on-chain ledger.
- An off-chain database will be provisioned to store non-critical application data, such as user profiles and interface settings, separate from the core operational data.
- The development and staging environments will be configured on local machine.

5.4 Testing and Validation

- A comprehensive testing strategy will be executed, encompassing unit, integration, and system-level testing. This strategy includes rigorous security audits, vulnerability scanning, and penetration testing.
- The system's resilience will be validated through simulated network stress scenarios, including node failures and denial-of-service attempts, to verify operational continuity.
- User Acceptance Testing (UAT) will be performed with key stakeholders to ensure all functional requirements and dashboard visualizations meet the specified criteria.

5.5 Deployment and Documentation

- Comprehensive project documentation will be produced, including the final SRS, System Design Document (SDD), test case reports, and a detailed user manual.
- The final, validated application will be deployed to a production-ready environment on the selected cloud platform.
- A final project report and presentation will be prepared to summarize the project's execution, key findings, and final outcomes.

6. HARDWARE & SOFTWARE REQUIREMENTS

The project will require the following:

6.1 Software Tools

- **Frontend**: React.js
- **Backend**: Node.js with Express.js
- **Blockchain**: Ethereum (Solidity-based smart contracts) or Hyperledger Fabric
- **Database**: Firebase/Supabase (off-chain record storage)
- **QR Code Utility**: qrcode or zxing libraries

6.2 Development and Testing Tools

- Visual Studio Code, Git/GitHub, Postman
- Cross-platform testing on web browsers and mobile-side QR compatibility

7. PROPOSED OUTCOMES

- A **secure system with no single point of failure**, designed to stay online and keep working even if one of the partners in the supply chain gets hacked.
- A **permanent and unchangeable log** of all actions taken on the platform, making the system's history completely trustworthy and easy to review.
- A network design that **contains cyberattacks**, so if one partner is compromised, the problem won't spread and disrupt the entire supply chain.
- Greater **trust between all supply chain partners**, because they can be confident that the platform is secure and always available, allowing business to continue without interruption.

Dr. Latesh Malik
Project Guide

8. REFERENCES

1. World Economic Forum, “Supply Chain Transparency–Key to Resilient and Responsible Procurement”, 2022.
2. IBM Food Trust – Blockchain Solutions, 2023.
3. Statista, "Global Counterfeit Goods Market Insights", 2023.
4. Ethereum Foundation, “Smart Contracts and ERC Standards”, 2022.
5. Hyperledger Fabric Documentation, The Linux Foundation, 2023.
6. QR Code Implementation using zxing, Google Developers, 2022.