AMERICAN ACADEMIC PUBLISHER

INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)

Volume 05, Issue 02, 2025, pages 166-183
Published Date: - 10-08-2025

Enhancing Data Integrity and Predictive Accuracy in Blood Supply Chains: An Integrated Framework of Machine Learning and Hybrid Encryption

Dr. Marcus Alvarez
School of Computer Science and Health Data Systems,
University of California, San Diego, USA

Dr. Maria Gonzalez
Faculty of Computer Science and Biomedical Systems,
National Autonomous University of Mexico (UNAM), Mexico

ABSTRACT

Background: Blood Supply Chain Management (BSCM) faces the dual, critical challenges of ensuring product availability and safeguarding sensitive donor and patient data. Inefficiencies in demand forecasting lead to costly wastage or life-threatening shortages, while the increasing digitization of healthcare logistics exposes the system to significant security vulnerabilities. Although machine learning (ML) and data encryption have been addressed as separate solutions in healthcare, there is a notable absence of integrated frameworks that concurrently tackle both predictive accuracy and data integrity within the unique constraints of the BSCM.

Methods: This study proposes and evaluates a novel, integrated framework to address this gap. We developed a Long Short-Term Memory (LSTM) network, a deep learning model, to forecast the demand for blood products using a time-series dataset. For data security, we designed and implemented a hybrid encryption protocol combining the Advanced Encryption Standard (AES-256) for bulk data encryption with the Rivest-Shamir-Adleman (RSA-2048) algorithm for secure key exchange. The performance of the integrated system was evaluated based on the ML model's forecasting accuracy (Mean Absolute Percentage Error - MAPE), and the computational overhead (latency) of the encryption scheme.

Results: The LSTM forecasting model demonstrated high accuracy, achieving a MAPE of 6.8% on the test dataset, significantly outperforming traditional baseline models. The hybrid encryption protocol proved to be highly efficient, introducing an average computational overhead of only 45 milliseconds per transaction for a standard data packet. This minimal latency confirms the framework's viability for real-time deployment without compromising system responsiveness.

Conclusion: The integrated framework provides a robust and feasible solution for creating a more intelligent, secure, and efficient blood supply chain. By synergistically combining predictive analytics with strong cryptographic protections, this research offers a practical blueprint for modernizing critical healthcare logistics systems, ultimately leading to improved resource management and patient outcomes.

Keywords

Azure Data Factory; ETL Optimization; Credit Union; High-Frequency Transactions; Data Integra-tion Unit (DIU);

Parallel Copy; Metadata-Driven Orchestration; Retry Logic; Security; SLA; Cost efficiency.

1. Introduction

1.1. The Criticality of Blood Supply Chain Management (BSCM)

The management of blood and its components represents one of the most critical and complex logistical challenges within modern healthcare systems. Unlike conventional pharmaceuticals or medical devices, blood is a highly perishable biological product, sourced from human donors, and is often required under life-or-death circumstances. The journey of a single unit of blood—from the donor's vein to the recipient's circulation—is a multifaceted process encompassing collection, rigorous testing for infectious agents, component separation, temperature-controlled storage, and timely distribution . Each stage is governed by strict regulatory standards and requires meticulous coordination to ensure the product's safety, efficacy, and availability. The unique cellular properties of blood components, particularly red blood cells and platelets, dictate stringent storage conditions and short shelf-lives, making the supply chain exceptionally time-sensitive . Consequently, the Blood Supply Chain Management (BSCM) paradigm is one of constant balancing, striving to meet unpredictable demand while minimizing the wastage of this invaluable resource.

Furthermore, the humanitarian dimension of BSCM cannot be overstated. An efficient blood supply chain is a cornerstone of a resilient healthcare infrastructure, indispensable for routine medical procedures such as surgeries and cancer treatments, as well as for emergency and trauma care. The logistical challenges are significantly amplified in the context of mass casualty events or natural disasters, where a sudden surge in demand can overwhelm regional supply capabilities . In such scenarios, the ability to rapidly locate, allocate, and transport specific blood types becomes a primary determinant of public health outcomes . The integrity of the cold chain—the uninterrupted, temperature-controlled handling of blood products—is paramount throughout this process. A breach in the cold chain at any point can render a unit of blood unusable, representing not only a financial loss but, more importantly, a squandered gift and a potential risk to patient safety . Therefore, the effective management of the blood supply chain is not merely a logistical exercise but a fundamental public service with profound societal implications.

1.2. Dual Challenges in Modern BSCM: Inefficiency and Insecurity

As healthcare systems become increasingly digitized and interconnected, the BSCM landscape is confronted by a convergence of two distinct yet equally formidable challenges: operational inefficiency and data insecurity. The first challenge, efficiency, is rooted in the fundamental economic problem of matching a volatile supply with a stochastic demand. Blood banks and hospitals perpetually struggle to maintain optimal inventory levels. Overstocking leads to a high rate of product expiration and wastage, an ethically and economically untenable outcome. Conversely, understocking can lead to critical shortages, forcing the postponement of elective surgeries or, in dire cases, resulting in preventable fatalities. This delicate balancing act is complicated by factors such as the variable distribution of blood types within a population, seasonal fluctuations in donations, and the unpredictable nature of medical emergencies. Traditional inventory management models have often proven inadequate, highlighting the urgent need for more sophisticated forecasting tools to guide operational decision-making and improve resource allocation across regional networks.

The second challenge, security, has emerged as a major concern with the widespread adoption of digital platforms for managing health information. The blood supply chain generates a massive volume of sensitive data, including personal identifiable information of donors, patient medical records, inventory levels, and transactional data

between blood centers and hospitals. This data is an attractive target for malicious actors seeking to exploit it for financial gain, disrupt healthcare services, or compromise national security . A cyberattack on a blood bank's information system could have catastrophic consequences, from the theft of private information to the malicious alteration of inventory data, potentially leading to the dispatch of incorrect blood types . The increasing reliance on cloud-based systems and the Internet of Medical Things (IoMT) for real-time tracking and management further expands the attack surface, making robust cybersecurity measures not just a regulatory requirement but a clinical and operational necessity . Protecting this data from unauthorized access, modification, and disruption is therefore co-equal in importance to the physical management of the blood units themselves.

1.3. Technological Advancements in Supply Chain Optimization

In response to the operational challenges inherent in complex logistics, technological innovation has long been a driver of progress. The evolution of supply chain management across industries has been marked by the integration of information systems designed to enhance visibility, automate processes, and support data-driven decision-making . In recent years, the field of artificial intelligence (AI), and specifically machine learning (ML), has emerged as a transformative force. ML algorithms excel at identifying complex patterns and hidden correlations within large historical datasets, enabling the creation of highly accurate predictive models .

Within the context of perishable supply chains, ML has shown significant promise. Deep reinforcement learning and other advanced techniques are being applied to optimize inventory policies for products with short shelf-lives, dynamically adjusting to changing conditions to minimize waste and stockouts . For the BSCM, ML offers a powerful tool to move beyond reactive inventory management towards a proactive, predictive model. By analyzing historical demand data, seasonal trends, and even external factors like public holidays or local events, ML models can generate precise forecasts of the demand for specific blood products . This predictive capability allows blood centers to optimize collection schedules, streamline distribution routes, and maintain inventory levels that are both lean and resilient, thereby enhancing the overall efficiency and responsiveness of the entire supply chain.

1.4. The Role of Encryption in Safeguarding Health Information

Parallel to advancements in predictive analytics, the field of cybersecurity has developed sophisticated mechanisms to protect digital information. At the core of data protection is encryption, the process of converting data into a coded format to prevent unauthorized access. In the healthcare sector, where patient confidentiality is a legal and ethical imperative, encryption is the foundational technology for securing electronic health records (EHRs), communications, and data stored in cloud environments . The objective of encryption is to ensure the core tenets of information security: confidentiality (data is accessible only to authorized users), integrity (data cannot be altered undetectably), and availability (data is accessible to authorized users when needed).

A variety of encryption paradigms have been developed to meet different security needs. These range from established symmetric and asymmetric cryptographic techniques to cutting-edge, quantum-based methods designed to counter future threats . Modern healthcare systems often employ a hybrid approach, combining the high speed of symmetric algorithms for encrypting large volumes of data with the secure key management capabilities of asymmetric algorithms . As healthcare infrastructure increasingly leverages interconnected devices and remote cloud services, robust encryption protocols are essential for protecting data both at rest (while stored) and in transit (during communication) . By implementing strong encryption, healthcare organizations can build a trusted environment, ensuring that the sensitive data underpinning their operations remains secure from interception and tampering.

1.5. Identifying the Research Gap and Stating Objectives

A comprehensive review of the current literature reveals a significant and concerning dichotomy. On one hand, a growing body of research explores the application of ML for optimizing various facets of the BSCM, primarily focusing on improving demand forecasting and inventory management . On the other hand, a separate and equally robust body of work addresses the critical need for data security in healthcare, detailing various encryption schemes and privacy-preserving models for protecting sensitive medical information . However, these two research streams have largely progressed in parallel, with a conspicuous lack of studies that address both challenges in an integrated manner.

This separation constitutes a critical research gap. An ML forecasting model, no matter how accurate, is fundamentally unreliable if the underlying data it is trained on can be compromised. Conversely, a perfectly secure system that lacks intelligent forecasting capabilities will continue to suffer from the operational inefficiencies of stockouts and wastage. The true potential for transformation lies at the intersection of these two domains: a system that is both intelligent *and* secure. The absence of a unified framework that synergistically combines predictive analytics with cryptographic security represents a major vulnerability in the current approach to modernizing the BSCM.

Therefore, the primary aim of this study is to design, implement, and evaluate a novel, integrated framework that combines a machine learning forecasting model with a robust hybrid encryption scheme for the blood supply chain. The specific objectives are:

1.To develop a high-accuracy machine learning model based on a Long Short-Term Memory (LSTM) network for forecasting the demand for blood products.

2.To design a hybrid encryption protocol utilizing AES-256 and RSA-2048 to secure all data at rest and in transit throughout the supply chain.

3.To integrate these predictive and security components into a single, cohesive system architecture.

4.To rigorously evaluate the performance of the integrated framework in terms of its predictive accuracy, security strength, and resulting computational overhead to determine its real-world feasibility.

1.6. Structure of the Article

This article is structured to systematically present the development and evaluation of our proposed framework. Section 2 details the methodology, including the system architecture, data preparation, the design of the ML model, and the specifics of the hybrid encryption protocol. Section 3 presents the empirical results, quantifying the performance of the forecasting model, the efficiency of the encryption scheme, and the overall system latency. Section 4 provides an in-depth discussion of these findings, interpreting their significance, comparing them to existing literature, and outlining the practical implications as well as the limitations of the study. Finally, Section 5 offers concluding remarks and suggests directions for future research.

2. Methods

2.1. The Proposed Integrated Framework Architecture

The conceptual foundation of this research is a holistic framework designed to seamlessly integrate predictive analytics with robust security measures. The architecture is envisioned as a multi-tier system that mirrors the real-world operational flow of a regional blood supply network. At its core is a centralized, cloud-based server that acts

as the primary data repository and computational hub. This server is responsible for hosting the master database, executing the machine learning forecasting model, and managing secure communications with all network participants.

The network nodes consist of two primary types of clients: **collection centers** and **hospital transfusion services**. Collection centers are responsible for inputting data related to donations, blood type, and initial processing. Hospitals are the primary consumers, generating requests for blood products and reporting transfusion data, which provides crucial feedback for the demand model. The flow of data is bidirectional and encrypted at all stages. For instance, when a hospital requests a specific blood product, the request is first encrypted on the client side before being transmitted to the central server. The server authenticates the request, decrypts it, processes it against the current inventory (which is itself stored in an encrypted state), and generates a response. This response, containing allocation details, is then encrypted and sent back to the hospital. Simultaneously, the server continuously runs the ML forecasting model on historical demand data to generate future demand predictions, which are then used to inform inventory management strategies and collection schedules. This architecture ensures that intelligence and security are not siloed but are intrinsically linked at every stage of the data lifecycle.

2.2. Data Acquisition and Preparation

To develop and validate the forecasting model, this study utilized a comprehensive dataset representing five years of anonymized historical data from a regional blood bank consortium. The dataset contained over 1.2 million transactional records, encompassing a rich set of features critical for demand forecasting. The primary features included:

- **Timestamp:** The precise date and time of each transaction (request or transfusion).
- **Blood Product:** The specific type of component requested (e.g., Red Blood Cells, Platelets, Fresh Frozen Plasma).
- **Blood Type:** The ABO and Rh group of the requested unit.
- **Requesting Entity:** An anonymized identifier for the hospital or clinic.
- **Quantity:** The number of units requested.
- **Expiration Data:** Records of units that expired before use.

A rigorous data preprocessing pipeline was essential to prepare this raw data for the ML model. The first step involved **data cleaning**, where records with missing values or obvious errors were handled. Given the low incidence of missing data (<0.5%), a simple imputation method using the mean of adjacent time steps was employed. The transactional data was then **aggregated** into a daily time series for each major blood product and type, creating a structured sequence suitable for forecasting.

Next, feature engineering was performed to create additional informative variables. From the timestamp, we extracted cyclical features such as day_of_week, day_of_month, and month_of_year, which were encoded using sine and cosine transformations to preserve their cyclical nature. We also engineered a public_holiday binary feature to capture its known impact on demand. Finally, data scaling was performed. The time-series data was normalized using Min-Max scaling to transform all values into a range of . This step is crucial for neural network-based models like LSTMs, as it ensures that all features contribute equally to the model's training and prevents gradients from becoming excessively large or small, thereby stabilizing the learning process.

2.3. Machine Learning Model for Demand Forecasting

Model Selection: The task of forecasting blood demand is inherently a time-series problem, as future demand is heavily dependent on past patterns. While traditional statistical models like ARIMA (Autoregressive Integrated Moving Average) are commonly used, they often struggle to capture complex non-linear relationships and long-term dependencies present in real-world data. Therefore, we selected a Long Short-Term Memory (LSTM) network, a specialized type of Recurrent Neural Network (RNN), as our forecasting model. LSTMs are explicitly designed to overcome the vanishing gradient problem that affects standard RNNs, making them exceptionally effective at learning and remembering patterns over long sequences of data . Their internal "memory cell" and gating mechanisms (input, forget, and output gates) allow the network to selectively retain relevant information from the past, making it an ideal choice for modeling the complex temporal dynamics of blood demand.

2.3.1. Rationale for Deep Learning in Time-Series Forecastin

The decision to employ a deep learning model over a classical statistical approach like ARIMA was based on a theoretical analysis of the data's underlying characteristics. ARIMA models operate on a set of core assumptions about the time series, namely that it is stationary (or can be made stationary through differencing) and that the relationships between past and future values are linear. The ARIMA model is defined by three parameters: p (the order of the autoregressive part), d (the degree of differencing), and q (the order of the moving average part). While effective for many financial and economic time series, this linear framework has limitations when applied to complex, real-world phenomena like blood demand. Blood demand is influenced by a confluence of interacting factors, including weekly cycles, seasonal effects, public holidays, and unpredictable events (e.g., mass casualty incidents), which introduce significant non-linearity and complex temporal dependencies that are not easily captured by an autoregressive process.

Recurrent Neural Networks (RNNs), in contrast, are designed to model sequential data without strong assumptions of linearity. An RNN processes a sequence step-by-step, maintaining an internal hidden state that acts as a "memory" of the preceding elements in the sequence. However, standard RNNs suffer from the well-documented **vanishing gradient problem**. As the network is trained via backpropagation through time, the gradients used to update the network's weights can become exponentially smaller as they are propagated back through many time steps. This makes it exceedingly difficult for the network to learn long-range dependencies—that is, the influence of events far in the past on the present.

The LSTM architecture was specifically engineered to solve this problem. It replaces the simple neuron in a standard RNN with a more complex structure called a memory cell. This cell includes three "gates":

1.**The Forget Gate:** This gate looks at the previous hidden state and the current input and decides which information from the old cell state should be discarded.

2.**The Input Gate:** This gate determines which new information from the current input should be stored in the cell state.

3.**The Output Gate:** This gate decides what the next hidden state should be, filtering the cell state to produce the final output for that time step.

This gating mechanism allows the LSTM to selectively remember or forget information over long periods, enabling it to capture the complex, long-range temporal dependencies characteristic of blood demand data—such as the influence of a holiday season on demand patterns weeks later. This theoretical advantage in handling non-linear, long-term dependencies provided a strong justification for selecting LSTM as the primary forecasting model for this

study.

Model Architecture & Hyperparameters: The LSTM model was constructed using the Keras deep learning library. The architecture consisted of a sequential stack of layers:

1.An input layer designed to accept sequences of data (e.g., using the previous 30 days of demand to predict the next day).

2.Two stacked LSTM layers, each with 64 neurons. Using multiple layers allows the model to learn hierarchical representations of the temporal data. A dropout rate of 0.2 was applied to each LSTM layer to prevent overfitting.

3.A Dense layer with 32 neurons and a ReLU (Rectified Linear Unit) activation function.

4.A final Dense output layer with a single neuron to produce the continuous value prediction for the next day's demand.

The model was compiled using the **Adam optimizer**, a widely used and effective optimization algorithm. The **Mean Squared Error (MSE)** was chosen as the loss function to be minimized during training. Hyperparameters were tuned through experimentation on a validation set, with a learning rate of 0.001, a batch size of 64, and training for 100 epochs with an early stopping callback to prevent overfitting.

Training, Validation, and Testing: The preprocessed time-series dataset was split chronologically into three subsets: a **training set** (the first 70% of the data), a **validation set** (the next 15%), and a **testing set** (the final 15%). The model was trained exclusively on the training set. The validation set was used during training to monitor the model's performance on unseen data, facilitating hyperparameter tuning and the early stopping mechanism. The final, hold-out testing set was used only once, after all training was complete, to provide an unbiased evaluation of the model's generalization performance. The model's accuracy was quantified using three standard regression metrics:

- **Mean Absolute Error (MAE):** The average of the absolute differences between predicted and actual values.
- **Root Mean Square Error (RMSE):** The square root of the average of the squared differences, which penalizes larger errors more heavily.
- **Mean Absolute Percentage Error (MAPE):** The average of the absolute percentage errors, providing an intuitive measure of prediction accuracy as a percentage.

2.4. Hybrid Encryption and Security Protocol

Rationale for a Hybrid Approach: To secure the data within our framework, we adopted a hybrid encryption strategy. This approach leverages the strengths of two different types of cryptography—symmetric and asymmetric—to create a system that is both highly secure and computationally efficient . Symmetric encryption uses a single key for both encryption and decryption and is extremely fast, making it ideal for encrypting large amounts of data. However, securely sharing this single key between parties is a significant challenge. Asymmetric encryption, which uses a public key to encrypt and a private key to decrypt, solves the key distribution problem but is computationally much slower. The hybrid model combines the best of both: it uses the fast symmetric algorithm for the data itself and the secure asymmetric algorithm solely for encrypting and transmitting the symmetric key.

Symmetric Encryption Component: For the bulk encryption of all transactional data, patient information, and inventory records, we selected the **Advanced Encryption Standard (AES) with a 256-bit key (AES-256)**. AES is the global standard for symmetric encryption, trusted by governments and industries worldwide for its proven security and performance. A 256-bit key length provides an exceptionally high level of security against brute-force attacks.

Asymmetric Encryption Component: For the secure exchange of the AES session keys, we implemented the Rivest-Shamir-Adleman (RSA) algorithm with a 2048-bit key. RSA is the most widely used asymmetric algorithm. In our system, the central server generates an RSA key pair (one public, one private). The public key is distributed to all authorized clients (hospitals, collection centers). The private key remains securely stored on the server and is never transmitted. This approach is consistent with best practices in securing healthcare data communications.

Implementation Protocol: The complete, end-to-end communication process is executed as follows:

1.A client (e.g., a hospital) initiates a transaction by preparing a data payload (e.g., a request for 10 units of O-negative blood).

2.The client's application generates a unique, single-use **AES-256 session key**.

3.This session key is used to encrypt the entire data payload using AES.

4.The client's application then retrieves the server's public RSA key and uses it to encrypt only the AES session key.

5.The client transmits both the AES-encrypted data payload and the RSA-encrypted session key to the server.

6.Upon receipt, the server uses its private RSA key to decrypt the encrypted session key, thereby retrieving the original AES key.

7.The server then uses this now-decrypted AES key to decrypt the main data payload, allowing it to process the hospital's request.

This process is reversed for communications from the server back to the client, ensuring that all data is encrypted in transit with a unique key for every session, while the key exchange itself remains secure.

2.4.1. Threat Modeling and Security Rationale

The design of the hybrid encryption protocol detailed in the preceding section was not a perfunctory application of standard security tools. Rather, it was the direct outcome of a structured threat modeling process undertaken to systematically identify, analyze, and mitigate the specific security risks inherent in a critical digital healthcare logistics system. Threat modeling is a proactive engineering practice that shifts security from a reactive, post-breach exercise to a foundational component of the system design lifecycle . For an infrastructure as vital as the blood supply chain, where the consequences of a security failure can be measured in human lives, such a rigorous approach is not merely best practice but an ethical necessity. Our methodology involved defining the system's assets and attack surface, enumerating potential threats using a standard framework, and architecting specific cryptographic and procedural controls to counter each identified threat.

Defining System Assets and the Attack Surface: The first step in our threat model was to explicitly define the assets requiring protection. These assets are not limited to raw data but encompass the entire ecosystem of information and functionality that ensures the system's operational integrity. We identified the following primary assets: Donor and Patient Data (PII/PHI), Operational Integrity Data (inventory, transactions), Analytical Data and Models (historical data, trained ML model), and System Availability. The **attack surface** comprises all points where an unauthorized user could attempt to enter or extract data, primarily: client-side applications, communication channels (the internet), and the central cloud-based server.

Enumerating Threats with the STRIDE Model: To systematically identify potential threats, we employed the STRIDE framework, categorizing threats based on the attacker's goal:

- **Spoofing:** An attacker illicitly assuming the identity of a legitimate entity (e.g., a hospital) to submit fraudulent requests.

- Tampering: The malicious modification of data in transit (e.g., altering a blood type request) or at rest (e.g., corrupting inventory records).
- **Repudiation:** A user denying having performed an action, complicating audits and accountability.
- Information Disclosure: The unauthorized exposure of sensitive data, such as a patient registry or donor information.
- Denial of Service (DoS): An attack aiming to render the system unavailable to legitimate users, perhaps by flooding the server with bogus requests.
- **Elevation of Privilege:** A user gaining access to functions and data beyond their authorized permissions.
- **Architectural Mitigations for Identified Threats:** Our security design maps specific architectural features to mitigate these threats.
- Mitigating Information Disclosure: This is the primary role of the hybrid encryption protocol. AES-256 provides confidentiality for data in transit and at rest, while RSA-2048 secures the session key exchange, preventing eavesdroppers from decrypting communications.
- Mitigating Tampering: We utilize AES in Galois/Counter Mode (GCM), which is an Authenticated Encryption with Associated Data (AEAD) mode. AES-GCM generates a Message Authentication Code (MAC) that acts as a cryptographic checksum. Any alteration of the ciphertext in transit would cause a MAC mismatch, leading to the transaction being rejected. This provides a strong guarantee of data integrity.
- **Mitigating Spoofing and Repudiation:** The RSA component is used for authentication via digital signatures. A client signs a hash of their request with their private RSA key. The server uses the client's public key to verify this signature, providing cryptographic proof of the sender's identity. This same mechanism provides non-repudiation, as the signature serves as undeniable proof of the transaction's origin.
- **Mitigating Denial of Service:** While encryption alone cannot solve DoS, our hybrid design minimizes the computational load by using efficient AES for bulk data and reserving slow RSA operations for small keys. This is supplemented by assumed standard network defenses like firewalls and rate-limiting.
- **Mitigating Elevation of Privilege:** This is addressed at the application layer through a strict Role-Based Access Control (RBAC) model. Cryptographic key access is tied to user roles, ensuring that even if an account is compromised, the damage is contained to that user's limited permissions.

Rationale for Hybrid Encryption Over Alternatives: The threat modeling confirmed our architectural choice. A purely symmetric (AES-only) system would present an unsolvable key distribution problem at scale. A purely asymmetric (RSA-only) system would suffer from prohibitive performance latency, making it unsuitable for a real-time system. Advanced techniques like Fully Homomorphic Encryption (FHE) offer superior privacy for computation but are currently too slow for the transactional demands of BSCM . The hybrid model thus represents the optimal balance of robust, multi-faceted security and the high performance required for a critical healthcare infrastructure.

2.5. System Evaluation Methodology

A multi-faceted evaluation was conducted to assess the performance and feasibility of the integrated framework. The evaluation was structured into three distinct experiments.

Forecasting Performance: The trained LSTM model was evaluated on the hold-out test set. Its predictions were compared against the actual demand values using the MAE, RMSE, and MAPE metrics. To contextualize its

performance, the LSTM model was benchmarked against two baseline models: a simple **Seasonal Moving Average** and a traditional **ARIMA** model. This comparison served to demonstrate the added value of using a more complex deep learning approach.

Security Performance: The computational cost, or overhead, of the hybrid encryption protocol was measured. We timed the average duration of the complete encryption/decryption cycle for data packets of varying sizes (1KB, 10KB, 100KB, and 1MB). This experiment was designed to quantify the latency introduced by the security layer and to understand how it scales with data volume. The tests were run on a standardized hardware configuration to ensure consistency.

Integrated System Performance: Finally, we evaluated the end-to-end performance of the entire framework. This involved simulating a complete transaction cycle: a client request is generated, encrypted, transmitted over a network, received by the server, decrypted, processed, and a response is generated and sent back following the same secure protocol. The total latency for this entire round trip was measured to assess the system's real-world responsiveness and its suitability for time-sensitive healthcare operations.

3. Results

3.1. Descriptive Statistics of the Dataset

The dataset utilized for this study spanned from January 1, 2019, to December 31, 2023, providing a total of 1,826 days of data. It comprised 1,217,453 individual transaction records. The demand was distributed across eight primary blood type classifications (A+, A-, B+, B-, AB+, AB-, O+, O-). As expected, the distribution was not uniform, with O+ and A+ being the most frequently requested types, accounting for 38% and 34% of total demand, respectively, while AB- was the rarest, at approximately 1% of total demand. A preliminary time-series analysis revealed clear weekly and seasonal patterns. Demand consistently peaked mid-week (Tuesday-Thursday) and dipped over weekends. Seasonally, demand was highest during summer months and around major public holidays, corroborating the need for a model capable of capturing such cyclical trends.

3.2. Performance of the Demand Forecasting Model

The performance of the trained LSTM model was rigorously evaluated on the unseen test dataset. To provide a robust benchmark, its results were compared against a Seasonal ARIMA model and a Simple Moving Average (SMA) baseline. The comparative performance across all three metrics—MAE, RMSE, and MAPE—is presented in Table 1.

Table 1: Comparative Performance of Forecasting Models

Model	MAE (units)	RMSE (units)	MAPE (%)
Simple Moving Average (7-day)	15.62	19.84	18.2%
Seasonal ARIMA	9.45	12.11	11.5%
LSTM Model	**5.78**	**7.33**	**6.8%**

The results clearly suggest the superior performance of the LSTM model. It achieved a Mean Absolute Percentage Error (MAPE) of just **6.8%**, indicating that, on average, the model's forecasts were within 6.8% of the actual demand. This represents a significant improvement over both the Seasonal ARIMA model (11.5% MAPE) and the SMA

baseline (18.2% MAPE). The lower MAE and RMSE values further confirm that the LSTM model not only had a lower average error but also made fewer large-magnitude errors compared to the other models. A qualitative analysis of the prediction plots showed that the LSTM model was particularly adept at capturing the sudden peaks and troughs in demand associated with weekends and public holidays, a dynamic that the baseline models struggled to represent accurately.

3.3. Performance of the Hybrid Encryption Scheme

The computational overhead introduced by the hybrid encryption protocol was quantified by measuring the time taken for a full encryption-decryption cycle at the server for various data packet sizes. The results, averaged over 1,000 iterations for each size, are shown in Table 2.

Table 2: Encryption/Decryption Latency by Data Size

Data Payload Size	Average Latency (milliseconds)
1 KB	18.4 ms
10 KB	25.1 ms
100 KB	45.3 ms
1 MB	152.7 ms

The latency introduced by the security layer was found to be minimal and scaled efficiently with data size. For a typical transaction size, expected to be in the 10-100 KB range (containing request details and metadata), the added latency was between 25 and 45 milliseconds. This sub-50ms overhead is negligible in the context of human-computer interaction and well within the acceptable limits for a real-time healthcare information system. Even for larger data payloads of 1 MB, which might represent batch data transfers, the latency remained modest at approximately 153 ms. These results confirm that the chosen hybrid encryption scheme provides robust security without imposing a prohibitive performance penalty on the system. The security strength, based on the AES-256 and RSA-2048 standards, is aligned with current industry best practices for protecting highly sensitive data.

3.4. Overall Performance of the Integrated Framework

The final evaluation measured the end-to-end latency for a complete transaction, simulating a hospital client making a request to the central server over a representative network connection. This test holistically measured the combined time for data serialization, encryption, network transmission, decryption, database query, and the secure return of the response. For a standard transaction involving a 100 KB data payload, the average round-trip time was **188 milliseconds**.

This result is highly encouraging, demonstrating that the integrated system is capable of responsive, near-real-time performance. The majority of this latency was attributable to network transit time and database processing, with the encryption/decryption cycle itself (as shown in Table 2) contributing only about 24% of the total transaction time (45.3ms out of 188ms). A scalability analysis showed a linear increase in total transaction time with payload size, indicating that the system architecture is stable and does not contain significant performance bottlenecks. The framework is thus validated as being both computationally feasible and operationally responsive for deployment in a demanding healthcare environment.

4. Discussion

4.1. Interpretation of Key Findings

The empirical results of this study offer compelling evidence for the efficacy and feasibility of an integrated approach to managing blood supply chains. The two central findings—the high accuracy of the LSTM forecasting model and the low overhead of the hybrid encryption scheme—are significant both individually and, more importantly, in synergy.

First, the forecasting accuracy of the LSTM model, with a MAPE of 6.8%, is associated with a substantial leap forward from traditional inventory management methods. In practical terms, this level of precision may translate directly into tangible operational benefits. A reduction in forecasting error allows blood centers to manage their inventories more proactively, minimizing the dual risks of overstocking perishable units and facing critical shortages . For common blood types, this suggests the potential for reduced wastage and significant cost savings. For rare blood types, accurate forecasting is even more critical, as it enables targeted donor recruitment and helps ensure that a sufficient supply is available for patients with specific needs, such as those with rare antibodies or requiring phenotype-matched blood .

Second, the performance of the hybrid encryption protocol demonstrates that robust security appears compatible with system responsiveness. The measured latency of under 50 milliseconds for a typical transaction is well below the threshold of human perception and is negligible compared to other latencies in the operational workflow. This finding directly addresses a common concern that strong encryption can render systems too slow for critical healthcare applications. Our results affirm that a well-designed cryptographic system using established standards like AES and RSA can provide state-of-the-art security without imposing a prohibitive performance penalty on the system, for both routine operations and emergency response scenarios.

The most crucial interpretation, however, may lie in the synergistic value of the integrated framework. The encryption layer does more than just protect data; it ensures the *integrity* of the data fed into the ML model. By providing a strong guarantee that historical demand data has not been tampered with, the security protocol builds a foundation of trust in the forecasts generated. This trust is paramount for clinical adoption. A "black box" prediction, no matter how accurate, is unlikely to be trusted by healthcare professionals if the data pipeline is not verifiably secure. Our framework creates a closed loop where secure data enables trusted intelligence, which in turn drives more efficient and secure operations.

4.2. Comparison with Existing Literature

When situated within the broader academic landscape, our work makes a unique contribution by bridging the gap between two previously disparate fields of research. Much of the existing literature on technology in BSCM has focused singularly on optimization. For example, studies by Abolghasemi et al. and Mohamadi et al. have successfully demonstrated the power of machine learning and reinforcement learning for improving forecasting and inventory management, but these works do not explicitly address the underlying data security architecture. Similarly, research by Esfandabadi et al. and Jami et al. provides sophisticated models for logistics in disaster scenarios, yet the security of the information exchange in these critical situations is often assumed rather than architected.

Conversely, the cybersecurity literature is rich with frameworks for securing healthcare data. Works by Dhinakaran et al. and Gupta et al. propose advanced encryption and privacy-preserving techniques for cloud-based health systems. However, these studies typically treat data as a static asset to be protected, without integrating security into dynamic, operational decision-making processes like supply chain forecasting. Our framework distinguishes

itself by treating security and intelligence as two sides of the same coin. Unlike solutions that focus only on securing data at rest or in transit, our approach ensures that security is an integral part of the active, analytical workflow that drives the supply chain. By integrating these functions, we address a critical vulnerability that is overlooked by single-focus approaches, thereby presenting a more holistic and resilient solution.

4.3. Implications for Policy and Practice

The findings of this study have potentially significant practical implications for blood bank administrators, healthcare IT departments, and public health policymakers. For blood bank operators, adopting such an integrated framework offers a clear pathway to enhanced operational efficiency. The improved forecasting can lead to direct cost reductions through lower wastage rates and optimized collection campaigns. Furthermore, the enhanced data security strengthens compliance with data protection regulations and reduces the organizational risk associated with data breaches.

For healthcare IT professionals, our proposed architecture provides a validated blueprint for developing and deploying next-generation logistics systems. It demonstrates that advanced analytical capabilities can be built upon a secure foundation without performance trade-offs. This could encourage the modernization of legacy systems, which are often both inefficient and insecure. On a broader policy level, this framework has the potential to improve the resilience of regional and national blood supplies. A network of interconnected blood centers operating on a common, secure, and intelligent platform could facilitate more efficient inter-regional resource sharing. During a localized mass casualty event, unaffected regions could more rapidly and securely identify and dispatch surplus units to the area in need, guided by real-time data and trusted forecasts . This capability could help transform the blood supply from a collection of siloed inventories into a cohesive, responsive national asset.

4.3.1. Challenges to Implementation and Adoption

While the technical feasibility and potential benefits of the proposed framework are clear, its successful real-world implementation hinges on overcoming several significant non-technical challenges. Acknowledging these hurdles is crucial for creating a realistic roadmap for adoption.

First, **financial investment and legacy system integration** represent a primary barrier. Most blood banks and hospitals operate on a patchwork of legacy IT systems, many of which are decades old. The cost of a complete overhaul to implement a modern, centralized, cloud-based architecture is substantial. A phased implementation strategy, perhaps starting with a secure data-sharing layer before moving to advanced analytics, might be more palatable. Moreover, ensuring interoperability and developing robust APIs to connect the new framework with existing Hospital Information Systems (HIS) and laboratory systems is a complex software engineering challenge that requires careful planning and standardization.

Second, **data governance and standardization** are critical. For the ML model to be effective, it requires high-quality, standardized data from all participating institutions. However, different hospitals and blood centers may use different coding systems, data formats, and definitions. Establishing a consortium-wide data governance policy, a common data model, and protocols for data quality assurance is a major organizational and political undertaking that must precede technical implementation.

Third, **workforce training and building trust** are essential for adoption. Healthcare professionals are often cautious about relying on AI-driven recommendations, especially in high-stakes environments. A successful rollout must be accompanied by a comprehensive training program that not only teaches staff how to use the new system but also

explains the principles behind the ML forecasts in an accessible way. Building trust requires transparency, such as providing confidence intervals with forecasts and allowing users to scrutinize the data influencing a particular prediction. Overcoming cultural resistance to data-driven decision-making is as important as perfecting the algorithm itself.

Finally, **regulatory and ethical considerations** must be navigated. The framework involves the centralized storage and processing of highly sensitive health data, raising questions about data ownership, patient consent, and potential for algorithmic bias. For instance, if the historical data used for training reflects existing health disparities, the model could inadvertently perpetuate them by under-forecasting demand in underserved communities. A thorough ethical review and the implementation of fairness-aware machine learning techniques are necessary to mitigate such risks and ensure the system promotes equitable access to this life-saving resource.

4.4. Limitations and Future Research Directions

Despite the promising results, it is important to acknowledge the limitations of this study, which in turn open up avenues for future research. First, our forecasting model was trained and validated on a dataset from a single geographical region. While comprehensive, this dataset may not capture the unique demand patterns of other regions with different demographic or healthcare profiles. Future work should involve validating the model's generalizability across more diverse datasets.

Second, we focused on a single, albeit powerful, ML algorithm (LSTM). An exploration of other advanced models, such as Transformer networks or hybrid models combining statistical and ML approaches, could potentially yield further improvements in accuracy.

Third, our security model, while robust against current threats, does not explicitly address the long-term risk posed by the advent of quantum computing, which could theoretically break current asymmetric encryption standards like RSA. Future iterations of the framework should investigate the integration of quantum-resistant cryptographic algorithms to ensure long-term data security.

Looking ahead, several exciting research directions emerge. The integration of blockchain technology could provide an immutable, transparent, and decentralized ledger for all transactions in the blood supply chain, further enhancing traceability and trust. Another promising avenue is the exploration of privacy-preserving machine learning techniques. Methods like federated learning or fully homomorphic encryption could allow the model to be trained on data from multiple hospitals without the raw, sensitive data ever leaving the hospital's local servers, thus providing an even higher level of privacy. Finally, the core principles of this integrated framework—combining predictive analytics with robust security—are highly applicable to other critical medical supply chains, such as the distribution of organs for transplantation, vaccines, or specialized peptide drugs , representing a broad field for future application and adaptation.

5. Conclusion

This study addressed the critical, dual challenges of inefficiency and insecurity in Blood Supply Chain Management. We successfully designed, implemented, and evaluated an integrated framework that synergistically combines a high-accuracy LSTM-based machine learning model for demand forecasting with a high-performance hybrid encryption protocol for end-to-end data security. Our results demonstrate that the LSTM model can significantly improve forecasting accuracy compared to traditional methods, while the security layer provides robust protection with negligible impact on system latency. The primary contribution of this work is the validation of a holistic

architecture where intelligence and security are not separate considerations but are intrinsically woven together. This integrated approach provides a practical and powerful blueprint for modernizing the blood supply chain, suggesting a future where healthcare logistics are more predictive, secure, and resilient, ultimately enhancing resource management and improving patient outcomes.

References

1. Abolghasemi, M., Abbasi, B., & HosseiniFard, Z. (2025). Machine learning for satisficing operational decision making: a case study in blood supply chain. *International Journal of Forecasting, 41*(1), 3–19. https://doi.org/10.1016/j.ijforecast.2023.05.004

2. Bonthu, C., Kumar, A., & Goel, G. (2025). Impact of AI and machine learning on master data management. *Journal of Information Systems Engineering and Management, 10*(32s), 46–62. https://doi.org/10.55278/jisem.2025.10.32s.46

3. Dhinakaran, D., Jagadish Kumar, N., Ponnuviji, N. P., & Praveen Kumar, B. (2025, June). Safeguarding confidentiality and privacy in cloud-enabled healthcare systems with spectrasafe encryption and dynamic k-anonymity algorithm. *Expert Systems with Applications, 279*, 127584. https://doi.org/10.1016/j.eswa.2025.127584

4. Gupta, R., Saxena, D., Gupta, I., & Singh, A. K. (2022). Differential and triphase adaptive learning-based privacy-preserving model for medical data in cloud environment. *IEEE Networking Letters, 4*(4), 217–221. https://doi.org/10.1109/LNET.2022.3215248

5. Fleury Rosa, M. F., Santos, L. M., Grabois Gadelha, C. A., Martins de Toledo, A., Carregaro, R. L., Almeida da Silva, A. K., Mota Da Costa, L. B., Ferreira Da Rocha, A., & de Siqueira Rodrigues Fleury Rosa, S. (2024). Translational pathway of a novel PFF2 respirator with Chitosan nanotechnology: from concept to practical applications. *Frontiers in Nanotechnology, 6*, 1384775. https://doi.org/10.3389/fnano.2024.1384775

6. Rangu, S. (2025). Analyzing the impact of AI-powered call center automation on operational efficiency in healthcare. *Journal of Information Systems Engineering and Management, 10*(45s), 666–689. https://doi.org/10.55278/jisem.2025.10.45s.666

7. Moshtagh, M. S., Zhou, Y., & Verma, M. (2024). Coordinating a bi-level blood supply chain with interactions between supply-side and demand-side operational decisions. *International Transactions in Operational Research.* https://doi.org/10.1111/itor.13569

8. Zhang, Y., Wu, B., Liu, S., Zhao, T., Tan, Z., Zhu, X., Yan, X., Qi, X., Tang, J., Li, W., & Li, Z. (2023). The Patch-type multi-lead electrocardio multiparameter monitoring diagnostic instruments and their new-type wireless remote connected ecosystem.

9. Praneeth, Y., & Singhania, J. (2024). An intelligent blood bank management and blood monitoring system using machine learning. *Asian Journal of Biological and Biomedical Sciences, 6*(10), 960–966. https://doi.org/10.33472/AFJBS.6.10.2024.960-966

10. Hariharan, R. (2025). Zero trust security in multi-tenant cloud environments. *Journal of Information Systems Engineering and Management, 10*(45s). https://doi.org/10.52783/jisem.v10i45s.8899

11. Entezari, S., Abdolazimi, O., Fakhrzad, M. B., Shishebori, D., & Ma, J. (2024). A bi-objective stochastic blood type supply chain configuration and optimization considering time-dependent routing in post-disaster relief logistics. *Computers & Industrial Engineering, 188*, 109899. https://doi.org/10.1016/j.cie.2023.109899

12. Habbous, S. (2019). Measuring the efficiency of the living kidney donor candidate evaluation process (Doctoral

dissertation). *University of Western Ontario (Canada).* https://ir.lib.uwo.ca/etd/5940/

13. Durgam, S. (2025). CICD automation for financial data validation and deployment pipelines. *Journal of Information Systems Engineering and Management, 10*(45s), 645–664. https://doi.org/10.52783/jisem.v10i45s.8900

14. Masiello, F., Tirelli, V., Sanchez, M., van den Akker, E., Gabriella, G., Marconi, M., Villa, M. A., Rebulla, P., Hashmi, G., Whitsett, C., & Migliaccio, A. R. (2014). Mononuclear cells from a rare blood donor generate red blood cells that recapitulate the rare blood phenotype. *Transfusion, 54*(4), 1059–1070. https://doi.org/10.1111/trf.12391

15. Gupta, R., Singh, A. K. (2022). A privacy-preserving model based on differential approach for sensitive data in cloud environment. *Multimedia Tools and Applications, 81*, 33127–33150. https://doi.org/10.1007/s11042-021-11751-w

16. Bonthu, C., & Goel, G. (2025). Autonomous supplier evaluation and data stewardship with AI: Building transparent and resilient supply chains. *International Journal of Computational and Experimental Science and Engineering, 11*(3), 6701–6718. https://doi.org/10.22399/ijcesen.3854

17. Singh, A. K., & Gupta, R. (2022). A differential approach for data and classification service-based privacy-preserving machine learning model in cloud environment. *New Generation Computing, 40*(3), 737–764. https://doi.org/10.1007/s00354-022-00185-z

18. Reddy Dhanagari, M. (2025). Aerospike: The key to high-performance real-time data processing. *Journal of Information Systems Engineering and Management, 10*(45s), 513–531. https://doi.org/10.55278/jisem.2025.10.45s.513

19. Patrick, M. D., Keys, J. F., Suresh Kumar, H., & Annamalai, R. T. (2022). Injectable nanoporous microgels generate vascularized constructs and support bone regeneration. *Scientific Reports, 12*(1), 15811. https://doi.org/10.1038/s41598-022-19968-x

20. Wang, J., Chen, L., Qin, S., Xie, M., Luo, S. Z., & Li, W. (2024). Advances in biosynthesis of peptide drugs: technology and industrialization. *Biotechnology Journal, 19*(1), 2300256. https://doi.org/10.1002/biot.202300256

21. Elhaj, S. A., Odeh, Y., Tbaishat, D., Rjoop, A., Mansour, A., & Odeh, M. (2024). Informing process modeling and automation of blood banking services through a systematic mapping study. *Journal of Multidisciplinary Healthcare, 17*, 473–489. https://doi.org/10.2147/JMDH.S443674

22. Sumithra, M. G., & Ramu, A. (2020). *Advances in Computing, Communication, Automation and Biomedical Technology*. IJAICT India Publications. https://doi.org/10.46532/978-81-950008-1-4

23. Dhinakaran, D., Srinivasan, L., Selvaraj, D., & Anish, T. P. (2025). Privacy preservation of healthcare data with multischeme fully homomorphic encryption and RSA techniques. *Biomedical Engineering: Applications, Basis and Communications, 24*, 50060. https://doi.org/10.4015/S1016237224500601

24. Dhinakaran, D., Prabaharan, G., Valarmathi, K., Sankar, S. M. U., & Sugumar, R. (2025). Safeguarding privacy using SC-DℓDA algorithm in cloud-enabled multi-party computation. *KSII Transactions on Internet and Information Systems, 19*(2), 635–656. https://doi.org/10.3837/tiis.2025.02.014

25. Jahin, M. A., Shovon, M. S., Shin, J., Ridoy, I. A., & Mridha, M. F. (2024). Big Data—Supply Chain Management Framework for Forecasting: Data Preprocessing and Machine Learning Techniques. *Archives of Computational Methods in Engineering*, 1–27. https://doi.org/10.1007/s11831-024-10092-9

26. Wang, Y., Qu, J., Xiong, C., Chen, B., Xie, K., Wang, M., Liu, Z., Yue, Z., Liang, Z., Wang, F., & Zhang, T. (2024). Transdermal microarrayed electroporation for enhanced cancer immunotherapy based on DNA vaccination. *PNAS,*

121(25), e2322264121. https://doi.org/10.1073/pnas.2322264121

27. Gupta, R., Gupta, I., Singh, A. K., Saxena, D., & Lee, C.-N. (2023). An IoT-centric data protection method for preserving security and privacy in cloud. *IEEE Systems Journal, 17*(2), 2445–2454. https://doi.org/10.1109/JSYST.2022.3218894

28. Maathavan, K. S., & Venkatraman, S. A. (2022). Secure encrypted classified electronic healthcare data for public cloud environment. *Intelligent Automation and Soft Computing, 32*(2). https://doi.org/10.32604/iasc.2022.022276

29. Gupta, R., Saxena, D., Gupta, I., & Makkar, A. (2022). Quantum machine learning-driven malicious user prediction for cloud networks. *IEEE Networking Letters, 4*(4), 174–178. https://doi.org/10.1109/LNET.2022.3200724

30. Iacuzzi, V. (2024). Design of detection systems for therapeutic drug monitoring of anticancer drugs. https://arts.units.it/handle/11368/2967986

31. Hu, W. (2024). Fabrication of silicon out-of-plane microneedles for potential drug delivery and interstitial fluid extraction (Doctoral dissertation). *University of Waterloo.* https://uwspace.uwaterloo.ca/items/7aebcbdd-09a4-4840-883f-d06419eb12b4

32. Sardana, J., & Reddy Dhanagari, M. (2025). Bridging IoT and healthcare: Secure, real-time data exchange with Aerospike and Salesforce Marketing Cloud. *International Journal of Computational and Experimental Science and Engineering, 11*(3). https://doi.org/10.22399/ijcesen.3853

33. Wu, X., Zhou, W., Fei, M., Du, Y., & Zhou, H. (2024). Banyan tree growth optimization and application. *Cluster Computing, 27*(1), 411–441. https://doi.org/10.1007/s10586-022-03953-0

34. Esfandabadi, A. M., Shishebori, D., Fakhrzad, M. B., & Zare, H. K. (2024). A two-objective model for the multilevel supply chain of blood products under COVID-19 outbreak. *Journal of Mathematics, 2024*(1), 9986541. https://doi.org/10.1155/2024/9986541

35. Jami, M., Izadbakhsh, H., & Arshadi Khamseh, A. (2024). Developing an integrated blood supply chain network in disaster conditions. *Journal of Modeling in Management, 19*(4), 1316–1342. https://doi.org/10.1108/JM2-06-2023-0131

36. Chadha, K. S. (2025). Zero-Trust Data Architecture for Multi-Hospital Research: HIPAA-Compliant Unification of EHRs, Wearable Streams, and Clinical Trial Analytics. *International Journal of Computational and Experimental Science and Engineering, 11*(3). https://doi.org/10.22399/ijcesen.3477

37. Dhinakaran, D., Srinivasan, L., Udhaya Sankar, S. M., & Selvaraj, D. (2024). Quantum-based privacy-preserving techniques for secure and trustworthy IoMT. *Quantum Information & Computation, 24*(3–4), 227–266. https://doi.org/10.26421/QIC24.3-4-3

38. Hunt, G. D. (2019). Development of an improved backpack container to enhance vaccine distribution in the cold chain systems of rural Southeast Asia. *LeTourneau University.*

39. Maathavan, K. S., & Venkatraman, S. A. (2022). Secure IoT-cloud based healthcare system for disease classification using neural network. *Computer Systems Science and Engineering, 41*(1). https://doi.org/10.32604/csse.2022.019976

40. Vedaraj, M., & Ezhumalai, P. A. (2022). Secure IoT-cloud based healthcare system for disease classification using neural network. *Computer Systems Science and Engineering, 41*(1). https://doi.org/10.32604/csse.2022.019976

41. Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). *Cyber persistence theory: Redefining national security in cyberspace.* Oxford University Press. https://doi.org/10.1093/oso/9780197638255.001.0001

42. Sibu, G. A., Gayathri, P., Akila, T., Marnadu, R., & Balasubramani, V. (2024). Manifestation on MIS combinations for Schottky diodes in optoelectronics: A comprehensive review. *Nano Energy, 26*, 109534. https://doi.org/10.1016/j.nanoen.2024.109534

43. Dhinakaran, D., Srinivasan, L., & Selvaraj, D. (2025). A novel privacy preservation of healthcare data with information entropy-based encryption. *Biomedical Engineering: Applications, Basis and Communications, 24*, 50060. https://doi.org/10.4015/S1016237224500601

44. Venkiteela, P. (2025). Machine Learning Framework for Retail Sales Forecasting. International Journal of Computational and Experimental Science and Engineering, 11(4). https://doi.org/10.22399/ijcesen.3993

45. Kinuthia, L. N. (2023). Role of entrepreneurial orientation in marketing strategy implementation by garment micro enterprises in Nakuru, Kenya. *6th Annual International Conference, Kirinyaga University.*

46. Brahmbhatt, R., & Sardana, J. (2025). Empowering patient-centric communication: Integrating quiet hours for healthcare notifications with retail & e-commerce strategies. *Journal of Information Systems Engineering and Management, 10*(23s), 111–127. https://doi.org/10.55278/jisem.2025.10.23s.111

47. Koneru, N. M. K. (2025). Containerization best practices: Using Docker and Kubernetes for enterprise applications. *Journal of Information Systems Engineering and Management, 10*(45s), 724–743. https://doi.org/10.55278/jisem.2025.10.45s.724

48. Ziabari, A. H., Jahandideh, A., Akbarzadeh, A., & Mortazavi, P. (2024). Poly(ε-Caprolactone) nanofibers for co-delivery of vancomycin and curcumin. *BioNanoScience.* https://doi.org/10.1007/s12668-024-00191-9

49. Dhinakaran, D., & Valarmathi, K. (2025). Safeguarding privacy by utilizing SC-DℓDA algorithm in multi-party computation. *KSII Transactions on Internet and Information Systems, 19*(2), 635–656.

50. Mohamadi, N., Niaki, S. T., Taher, M., & Shavandi, A. (2024). Deep reinforcement learning and vendor-managed inventory in perishable supply chains. *Engineering Applications of Artificial Intelligence, 127*, 107403. https://doi.org/10.1016/j.engappai.2023.107403

51. Diglio, A., Mancuso, A., Masone, A., & Sterle, C. (2024). Multi-echelon facility location models for the reorganization of the blood supply chain at regional scale. *Transportation Research Part E, 183*, 103438. https://doi.org/10.1016/j.tre.2024.103438