Securing Drug Traceability: Block chain-Enhanced Privacy Protection and Anti-Counterfeit Measures in Pharmaceutical Supply Chains

Abdulrahman Mohammed Alshehri[1] , Thamer Alhussain[2,*]

[1]Industrial Engineering Department, Penn State University, University park, State college, USA
[2]E-Commerce Department, Saudi Electronic University , Kingdom of Saudi Arabia

Emails: ama8889@psu.edu; talhussain@seu.edu.sa

Abstract

The pharmaceutical industry encounters numerous challenges in the management of medications and ensuring their authenticity, as well as safeguarding sensitive information within the supply chain. Maintaining the integrity of drug manufacturing processes, transaction records, and patient data from unauthorized access or tampering is crucial. Any breach in security could undermine trust throughout the entire supply chain. To mitigate these concerns, a multi-layered approach is employed. Initially, data encryption using QR codes with Attribute-Based Encryption provides a foundation for securing information. This is followed by an innovative strategy that combines Red Panda Optimization (RPO) Algorithm and Group Teaching Optimization algorithms (GTOA) to optimize encryption key selection. Finally, Multi-Party Computation (MPC) protocols along with Shamir's Secret Sharing enhances overall security measures. These procedures ensure that only authorized individuals have access to critical information essential for identifying counterfeit products and maintain confidentiality through Secure MPC verification without compromising sensitive details.

Keywords: Counterfeit Drugs; Drug Traceability; Security; Privacy; Block chain; Key Generation; Optimization

1. Introduction

The pharmaceutical industry in recent years emphasizes the use of rigorous tracing systems to ensure the safety and reliability of drugs [1-5]. This not only prevents the sale of counterfeit medicines but also facilitates quick recalls of products with quality problems or safety issues [6-12]. After the medicines are made, they follow many paths until they reach the final consumers. This happens because, in order to get to the people who need them, drugs have to move from factories to storage places, through various distributors and pharmacies, hospitals, and other healthcare facilities [13]. To destabilize this confusing network of products and transactions, it is necessary to work with a specific system to understand where each item comes from and who previously owned it. The use of digital technology in this matter helps with government requirements and ensures the safety of medications in general [14-16]. More and more people become the victims of counterfeit medicines, owing to the presence of some in the pharmaceutical market. This puts citizens' health in danger [17].

In today's pharmaceutical industry, it's really important to have a system for tracking drugs that puts security and keeping information private at the top of the list. This is different from older methods that used centralized databases, which had problems with leaks and privacy. Instead, this method makes sure that private info is kept safe and the drug distribution network stays authentic [18, 19]. In the rapidly evolving pharmaceutical industry of today, ensuring top-notch security and privacy for drug tracking systems is crucial. Traditional methods relied on centralized databases which unfortunately faced issues with leaks and maintaining privacy. The proposed approach aims to address these challenges by prioritizing the protection of private information and keeping the drug distribution network authentic [20].

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

The contributions are:

- With encrypted QR codes, data encryption uses a technology called Attribute-Based Encryption (ABE). This crucial step ensures data privacy and controlled access. ABE lets the system control who can see product details based on the-ir roles and attributes. Only approved personnel with the right attributes can decrypt and access sensitive counterfeit detection data. ABE adds extra security by encrypting data so access depends on specific rules or policies. This robust protection guards sensitive pharmaceutical supply chain information.
- Hybrid optimization algorithm enhance the process of generating encryption keys, leading to better performance in terms of encryption and decryption speeds. This ultimately improves the efficiency and responsiveness of a drug traceability system. By combining exploration and exploitation techniques, the proposed algorithm ensure that the encryption keys generated are strong against attacks and offer a higher level of security compared to conventional methods.
- Multi-Party Computation (MPC) protocols blend with data encryption. They allow safe calculations on hidden info. This matters for checking drug genuineness and analysis tasks. With MPC, multiple parties compute jointly without sharing inputs individually. MPC empowers the system to capably calculate on encrypted data while securing it. This boosts counterfeiting detection and prevention abilities within medicine supply chains.
- Shamir's Secret Sharing splits a key into multiple pieces. These portions get shared with various parties. A certain number must come together to rebuild the original key. This method is crucial for safely distributing decryption keys within the Pharmaceutical Supply Chain. Only authorized personnel can access keys needed for counterfeit detection data. By requiring multiple shares, the risk of key exposure decreases and unauthorized access becomes less likely. Data security improves, strengthening the integrity of drug traceability systems.

The rest of the paper is divided into four main sections. The section 2 gives review of literature. Section 3 details the proposed methodology. Section 4 showcases experimental findings. Lastly, section 5 concludes the study and potential areas for future research.

2. Related Work

Block chain technology was introduced by the authors in [21] to ease product tracking in healthcare supply chains and address issues with current tracing systems, such as security risks and counterfeit medications. They proposed using block chain to enhance transparency, security, and reliability throughout the supply chain through a decentralized ledger that cannot be altered. The authors also emphasized the importance of striking a balance between transparent data and privacy protection while ensuring the safety of sensitive information. In another study [22], Non-Fungible Tokens were employed to provide each drug product with a unique digital representation, along with utilizing Internet of Things devices for real-time data collection across the supply chain. This combination is designed to offer transparency, security, and authenticity at every stage of the drug's journey.

Developed by Tan et al. [23], the MB-BC system tracks drugs using a unique type of block chain with multiple branches to ensure secure and traceable drug information. Unlike other block chains, MB-BC has precise access controls that allow for safe data sharing between different users with varying levels of access within the system. This enhances data security and privacy. This is crucial in fighting fake drugs and maintaining sensitive information safety while also facilitating easier drug tracking. PHTrack [24], another solution designed to track and prevent the spread of counterfeit medications, utilizes hyper ledger Sawtooth efficiently for reliable performance. It implements extra secure ways for network communication on hyper ledger sawtooth nodes, ensuring more secure data exchange. By integrating advanced features of hyper ledger Sawtooth along with quantum-safe communication protocols, supply chain traceability is enhanced.

In [25], the authors used smart contracts on the Ethereum blockchain to track counterfeit drugs. Because of this, every step in the pharmaceutical supply chain is securely recorded and can be checked. Their BBTCD method is decentralized as it stores data on the InterPlanetary File System. This storage method is more transparent and cost-effective because it removes the need for central data centers and lowers the risk of data tampering or alteration.

Bandhu et al. [26] introduced an Ethereum blockchain technology to make the healthcare supply chain better. This approach makes things more secure, clear, and efficient by using smart contracts and making data unchangeable. This creates a reliable tracking system in the supply chain. The system uses Ethereum blockchain as a transparent ledger for storing data securely with hash functions. In their 2022 study, Atassi and Alhosban [27] propose a fusion optimization and classification model that leverages blockchain technology to enhance security, efficiency, and data integrity in healthcare systems. The model improves data processing and classification accuracy while ensuring secure, decentralized healthcare data management. Yugal et al. [28] propose an IoT-based emulated

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

performance evaluation NLP model designed for advanced learners in Academia 4.0 and Industry 4.0 environments. The model enhances learning outcomes and performance assessments by integrating IoT with advanced NLP techniques. Zaki et al. introduce an Interval Valued Neutrosophic VIKOR method for evaluating green suppliers in supply chains. This method enhances decision-making by addressing uncertainty and imprecision in supplier assessments using neutrosophic sets.

3. Proposed Methodology

3.1. Product flow in current drug supply chain

The intricate pharmaceutical supply chain in Bangladesh affects medicine quality, appropriate use, and efficient regulatory supervision. All five types of medicine allopathic, ayurveda, homoeopathic, herbal, and unani are governed by the Directorate General of Drug Administration (DGDA), which also sets prices, inspects all facilities, and performs post-marketing surveillance. This appears to be crucial given the World Health Organization's (WHO) discovery that low-quality medications tend to spread in situations with little ability for regulation, a large demand for medications, low cost and availability, and the influence of moderate medications [41]. The product flow in the current drug traceability system, shown in Figure 1, is summarized below.

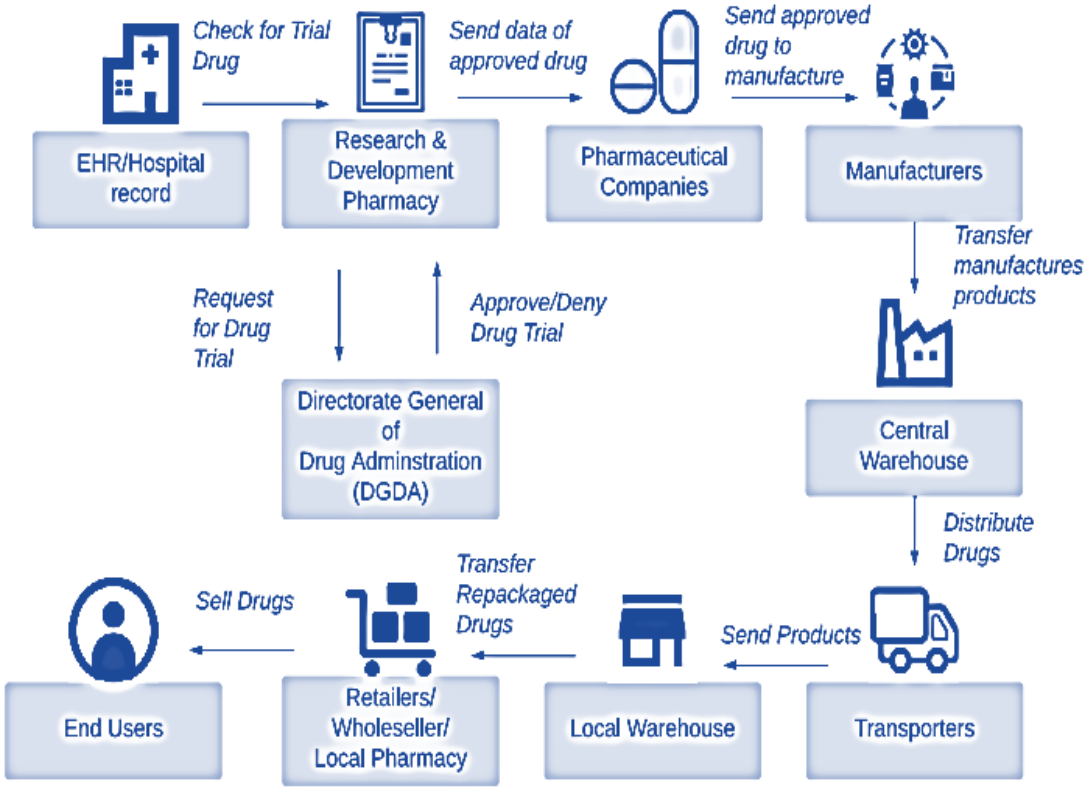


Figure 1. The order in which the current system operates.

- To start a drug study, a clinical research facility gathers information from medical records.
- The nation's drug regulatory agency (DGDA) next decides whether to approve or reject the drug that was tested.
- The manufacturers receive approved drug items from pharmaceutical companies. The final goods are then transferred to a central warehouse, where they are packaged and sent to nearby warehouses.
- Retail pharmacies, wholesalers, and other local pharmacies will handle the repackaged medications. Lastly, local suppliers will process the new negotiated pricing to deliver the medications to the final customers.

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

However, many dishonest individuals, unregistered sellers, and businesses in this stock market are willing to take shortcuts (and overlook issues with product efficacy) to make money. The state of affairs is bad, with unscrupulous wholesalers and middlemen willing to buy stolen items, fabricate pedigree documents, and sell the commodity to unsuspecting pharmacies for full retail value.

3.2. Key challenges of current system

Issues with the pharmaceutical supply chain have recently been a major cause of worry for the company, as Figure 2 illustrates. The intricate relationships among stakeholders mean that the issues are still very much prevalent. In addition, this pandemic affected nearly every part of the industry and had a significant economic impact on the world. Some of the main challenges in addressing the issue of counterfeit medications include the following:

Lack of Transparency: One of the most common issues that arises is the challenge of identifying the root cause of an issue. Transparency is undermined when pharmaceuticals are delivered in unsuitable condition for human consumption, when a shipment contains a counterfeit drug, or when expenses rise for no obvious reason. **Rules and Adherence:** The most recent Quality System Practices must already be adhered to by the pharmaceutical distribution system. Conversely, regulations are subject to frequent modifications. Businesses will progressively have to enhance their supply chain and customs management as well as internal control to meet new levels.

Raw Material Scarcity: In the event of a pandemic, ineffective planning could lead to a number of issues with the procurement of raw materials. It can take a while to determine production time and precise inventory levels in the absence of a guide document as they attempt to generalise data and understand the supply timetable. **Fast Drug Delivery:** Historically, there has been a race against time to get pharmaceuticals onto the market. Efficient handling of pharmaceutical operations and supply chain management is necessary to minimize bottlenecks and potential errors throughout these testing times.

Inventory management: Maintaining control over inventory to prevent fluctuations is another issue.

Technology bottlenecks are common: The pharmaceutical industry has been hesitant and cautious in embracing innovation. Even though the last ten years have seen tremendous

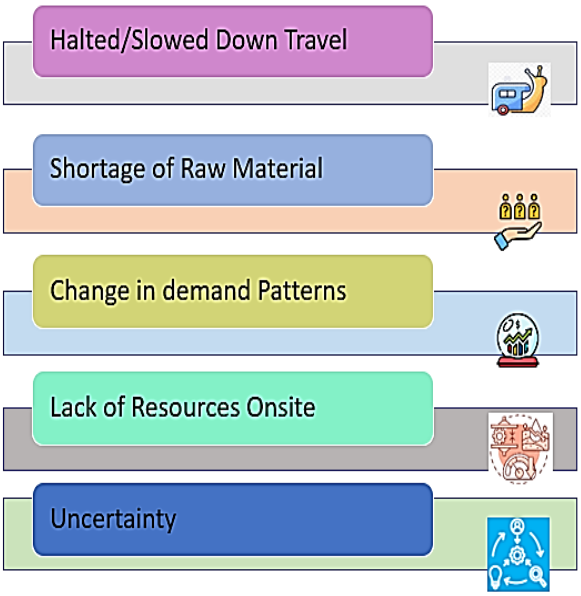


Figure 2. Obstacles in the Pharmaceutical Supply Chain.

In Figure. 2, the manufacture side log in to a platform where they upload and oversee their production data independently. On the other hand, the user side get the encrypted product details upon request. The authenticity of the data is checked by MPC. The decentralized system allows for easy monitoring and safeguarding of data integrity, making it simpler to trace and regulate drug supply chains.

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

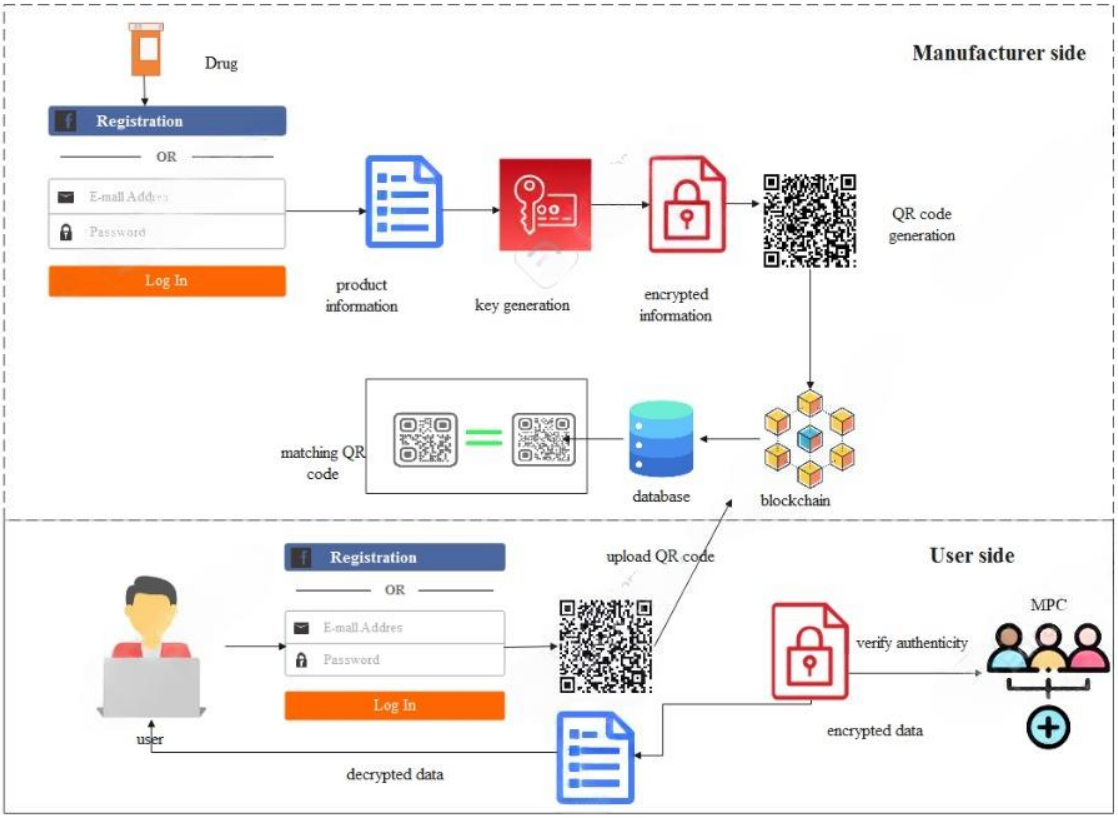


Figure 3. Architecture of the proposed methodology

4. System Entities

(i) Pharmacist (PH):
Pharmaceutical companies enter drug information with special codes, which helps them organize data easily and independently. This setup makes it easier to track drugs and protect data. Pharmacist (PH) is a crucial endpoint whose job it is to verify if medications are authentic before giving them to patients. By comparing the unique medicine ID with the transaction history recorded in the blocks, the chemist can ensure the medication's legal status and track its journey from the manufacturer to the pharmacy using the block chain's specialized tools. By securely accessing and recording the block chain, this position not only increases the efficacy of the fight against fraudulent pharmaceuticals but also protects patient data privacy.

(ii) Drug Sellers (S):
Drug distributors make sure that people get their medicine safely and legally. They don't just sell drugs they also help keep track of where the medicines go by working with supply chains. Being part of this program allows drug sellers to get detailed information about different medications. Pharmacies, hospitals, and other healthcare facilities that dispense drugs to customers are important entities known as drug sellers (S). Because of the block chain technology, they are able to follow any changes in ownership and ensure that the pharmaceuticals come from the right place. It helps in the battle against fake medications by guaranteeing that each product's origin can be tracked and that the supply chain is unaltered. Additionally, by implementing the block chain system which is utilized by drug dealers it guarantees data privacy and restricts access to authorized members only.

(iii) Patients (P):
Patients (P) benefit a lot in the system since they are the end users of pharmaceutical products through enhanced transparency and security of the product. By accessing the block chain platform, the patients will be in a position to verify the authenticity of the prescription drugs and be certain they are being provided with original products. Also, patients have secure data to their records and related information through the block chain while they have a privacy assurance which in turn increases the public trust of the healthcare industry. Through traceability, patients can be more comfortable with the safety and standard quality of such treatment since the risk of fakes is considerably narrowed. Ensuring the safety and well-being of patients should be our top priority in the pharmaceutical supply chain. It's important for the traceability system to focus on monitoring these key aspects. Providing patients with personalized identification helps they confirm that the medications they've bought are

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

genuine. By using the drug code on the packaging, patients can track where their medicine came from, making sure it's safe and real.

(iv) Medical representative
The medical representative is an important link responsibility of communicating pharmaceutical firms and healthcare practitioners. The medical representative ensures the visibility of all the promotional activities, drugs samples and all the educations materials by the use of the block chain technology. This is useful in controlling the circulation of counterfeit products through tracking the circulation of medicine samples, and hence, building credence amongst healthcare professionals. Besides keeping a secret any information disclosed during interactions, they can also guarantee compliance with industry rules due to the effective data protection features of the block chain. They mainly work to promote and educate healthcare providers about various pharmaceutical products like medicines, medical devices, and treatments.

4.2. Security Model

(i) Trust Assumptions:
PH and S are seen as entities within the system that are partially reliable due to various factors:

Pharmaceutical companies guard their drug-making processes closely since this valuable information gives them a competitive advantage. Although these companies are typically seen as reliable in handling and producing this data, there is still a risk of misuse or unethical behavior. Collaboration between pharmaceutical companies and drug sellers poses a potential danger to the fair and unbiased distribution of drugs. This collusion allows certain parties to manipulate the market, which can ultimately harm consumers.

4.3 System Model:
Block chain technology, enhanced with Cipher text-Policy Attribute-Based Encryption (CP-ABE) and smart contracts, revolutionizes drug traceability by bolstering security and privacy. This innovative combination leverages advanced encryption and decentralized logic execution to protect sensitive data and foster fair competition among pharmaceutical companies. It establishes a secure and equitable environment for all parties involved in the pharmaceutical supply chain.

4.3.1 Key Generation Phase
RPO and GTOA algorithms are combined to select the optimal encryption key for enhanced security. In the Key Generation Phase, special secret keys are generated using hybrid optimization algorithm for authorized users to access the system using advanced optimization techniques. As the number of users and attributes grows, key generation in ABE systems becomes more intricate.

4.3.1.1 Group Teaching Optimization Algorithm
The GTOA is designed to enhance the overall understanding of the entire class through simulating group teaching methods. However, implementing group teaching in reality can be complex due to individual differences among students. To make group teaching an effective optimization strategy, we analogize the population, decision variables, and fitness value to students, subjects, and knowledge respectively.

In GTOA, the population is like the student group. Likewise, in key generation, the population is similar to the group of possible solutions or potential keys. The decision variables in GTOA are like the courses or subjects offered to students. In key generation, decision variables are comparable to the characteristics or properties used to create and identify potential keys. The fitness value in GTOA indicates students' understanding in different subjects. Similarly, in key generation, the fitness value is a measure of how well a candidate key meets certain criteria for quality and effectiveness.

The fitness is determined by Eqn. (1).

$$Fit = wt_1 \cdot En(Ky) + wt_2 \cdot Dv(Ky) \tag{1}$$

where $En(Ky)$ and $Dv(Ky)$ are the entropy and diversity of the key. wt_1 and wt_2 signifies their weights.

Ability grouping phase: In the ability grouping phase, it's assumed that the knowledge of the entire class follows a normal distribution

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

$$f(y)=\frac{1}{\sqrt{2\pi\lambda}}e^{\frac{-(y-v)^2}{2\lambda^2}} \tag{2}$$

When evaluating students' knowledge y, we consider the average knowledge of the class v and its variability (standard deviation, λ). A wider spread (larger λ) indicates greater variation in knowledge. Effective teachers focus on both raising the average knowledge (v) and reducing variability (λ). To accomplish this, teachers must develop appropriate teaching strategies tailored to their students' needs.

(i) Teacher phase

In the "teacher phase" of an optimization process, the optimization algorithm, comparable to a teacher, guides and educates the solutions, analogous to students. In the case of key generation, the optimization algorithm works with the potential solutions to continually enhance and refine them, similar to how a teacher helps improve students' understanding.

Teacher phase 1: Just like a teacher focuses on helping their best students excel, optimization algorithms concentrate on refining the candidate keys that show the most promise. They do this by investing more effort in improving the quality of those candidates, such as those with higher performance or better security features.

$$Y_{teacher,i}^{I+1}=Y_i^I+b\times\left(K^I-Fc\times\left(c\times AK^I+d\times Y_i^I\right)\right) \tag{3}$$

$$AK^I=\frac{1}{M}\sum_{i=1}^{M}Y_i^I \tag{4}$$

$$c+d=1 \tag{5}$$

where I represents the current iteration or time point. M is the total number of students. Y_i^I Signifies the knowledge level of student i at time I. K^I denotes the teacher's knowledge level at time I. AK^I Represents the average knowledge level of the group at time I. Fc is a teaching factor that influences the teacher's effectiveness. $Y_{teacher,i}^{I+1}$ indicates the knowledge gained by student i at time I through learning from the teacher. b,c,and,d are random numbers between 0 and 1.

Teacher phase 2: During Phase II of the teaching process, emphasis shifts from the top performers to the middle tier. Similarly, in cryptography, optimization algorithms prioritize finding better keys for average or struggling candidates. The goal is to improve the quality of keys that may not be outstanding but have room for improvement. By focusing on the average group, the algorithm aims to boost the overall performance of the key population and reduce differences in key quality.

$$Y_{teacher,i}^{I+1}=Y_i^I+2\times e\times\left(K^I-Y_i^I\right) \tag{6}$$

where e signifies random value between 0 and 1:

Not all students may learn during the teacher phase. This can be resolved by:

$$Y_i^{I+1}=\begin{cases}Y_{teacher,i}^{I+1}, & f\left(Y_{teacher,i}^{I+1}\right)<f\left(Y_i^I\right)\\ Y_i^I, & f\left(Y_{teacher,i}^{I+1}\right)\geq f\left(Y_i^I\right)\end{cases} \tag{7}$$

(ii) Student phase: During the student phase, students (potential solutions) learn independently and discuss with classmates to improve their understanding. Likewise, in key generation, potential solutions can self-improve

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

(through techniques like local search) and share ideas with others (through methods like crossover or information exchange) to increase their quality.

$$Y_{student,i}^{I+1}=\begin{cases}Y_{teacher,i}^{I+1}+g\times\left(Y_{teacher,i}^{I+1}-Y_{teacher,j}^{I+1}\right)+h\times\left(Y_{teacher,i}^{I+1}-Y_i^I\right), f\left(Y_{teacher,i}^{I+1}\right)<f\left(Y_{teacher,j}^{I+1}\right)\\ Y_{teacher,i}^{I+1}-g\times\left(Y_{teacher,i}^{I+1}-Y_{teacher,j}^{I+1}\right)+h\times\left(Y_{teacher,i}^{I+1}-Y_i^I\right), f\left(Y_{teacher,i}^{I+1}\right)\geq f\left(Y_{teacher,j}^{I+1}\right)\end{cases} \quad (8)$$

For any two random numbers g and h between 0 and 1: $Y_{student,i}^{I+1}$ represents the knowledge of student i at time $I+1$ gained from other students. $Y_{teacher,j}^{I+1}$ represents the knowledge of student j at time $I+1$ gained from the teacher. Student j is randomly selected from the group of all students except for student i.

$$Y_i^{I+1}=\begin{cases}Y_{teacher,i}^{I+1}, & f\left(Y_{teacher,i}^{I+1}\right)<f\left(Y_{student,i}^{I+1}\right)\\ Y_{student,i}^{I+1}, & f\left(Y_{teacher,i}^{I+1}\right)\geq f\left(Y_{student,i}^{I+1}\right)\end{cases} \quad (9)$$

After a learning cycle, student i's knowledge at time $I+1$ is denoted as Y_i^{I+1}.

(iii) Teacher allocation phase

In the teacher allocation phase, using the established fourth rule, it is crucial to create an effective teacher allocation mechanism to enhance student learning. Similar to GWO, where the top three candidates are retained to direct the wolves' hunting, the suggested technique employs this idea. As a result, the following equation represents teacher allocation in the proposed method:

$$K^I=\begin{cases}Y_{first}^I, & f\left(Y_{first}^I\right)\leq f\left(\dfrac{Y_{first}^I+Y_{second}^I+Y_{third}^I}{3}\right)\\ \dfrac{Y_{first}^I+Y_{second}^I+Y_{third}^I}{3}, & f\left(Y_{first}^I\right)>f\left(\dfrac{Y_{first}^I+Y_{second}^I+Y_{third}^I}{3}\right)\end{cases} \quad (10)$$

To improve the efficiency of the GTOA algorithm, the top three students (Y_{first}^I, Y_{second}^I, and Y_{third}^I) are assigned the same teacher. This allows the top students to share knowledge and guidance, accelerating the algorithm's learning process.

4.3.1.2 Red Panda Optimization

As the optimization process begins its exploration phase, the algorithm sets out to thoroughly examine the possible solutions available. Similar to the way red pandas seek out food, the algorithm ventures into areas of the solution space that show promise for delivering better results. By doing so, it strives to identify strong candidate keys that will optimize the objective function. Similar to how red pandas use their senses to find food, the optimization algorithm uses different methods to locate areas in the solution space that might contain suitable solutions.

(i) Exploitation

Much like red pandas searching for food, the optimization method identifies areas where they're likely to find good solutions. Just as red pandas adjust their climb position to find the best path, the algorithm adjusts its search directions. The algorithm evaluates different possibilities, similar to how a red panda assesses its surroundings, and if it finds a better outcome, it will follow that path. If a change in position results in a better outcome, the pandas will update their location accordingly. Similarly, when generating keys, the optimization algorithm will replace the current key with an improved solution if it proves to be more effective.

$$y_{i,j}^{P2}=y_{i,j}+\frac{LB_j+s\cdot\left(UB_j-LB_j\right)}{I} \quad (11)$$

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

$$Y_i = \begin{cases} Y_i^{P2}, & F_i^{P2} < F_i \\ Y_i, & else, \end{cases} \tag{12}$$

where Y_i^{P2} signifies the updated location of the i^{th} red panda after the second phase of the RPO algorithm. $y_{i,j}^{P2}$ represents the j^{th} coordinate of this updated location. F_i^{P2} denotes the objective function value for this updated location. s denote a random value between 0 and 1.

4.3.1.3 Hybrid optimization

When the RPO and GTOA work together, they do a better job of creating keys to fight counterfeit drugs in the pharmaceutical supply chain. The RPO looks for new possibilities while the GTOA focuses on making the most of those opportunities. This combined approach helps find the best solutions while also keeping different options open. By balancing exploration and exploitation, it makes sure resources are used wisely to pick the best encryption keys.

Algorithm 1: Hybrid optimization

Input:
Population size P
Maximum iterations $I_{\max}$
Output:
Optimized encryption key
Initialization:
1. Initialize population of candidate keys randomly
2. Set parameters: population Size, $I_{\max}$
Exploration Phase (GTOA):
3. while ($I < I_{\max}$):
4. Evaluate fitness of each candidate key using objective function (Eqn. 1)
5. Implement GTOA for exploration:
   a. Ability grouping phase
   b. Teacher phase 1
   c. Teacher phase 2
   d. Student phase
Exploitation Phase (RPO):
6. Use RPO for exploitation:
Update and Improvement:
7. Replace keys with improved solutions from both exploration and exploitation phases
8. Evaluate fitness of updated population using Eqn. (1).
9. $I + 1$
Repeat until convergence criteria met or maxIter reached

4.3.2 Data Encryption Phase

Attribute-based encryption is like a digital lock that only lets people with specific jobs, affiliations, or security clearances in. So when something is locked up using ABE, only the right kind of people can open it and see what's inside. This keeps data safe and private by making sure only the right people can get access to the information.

Pharmaceutical company utilizes ABE to secure product details and hide them within QR codes on their packaging. Only authorized personnel, like regulators or supply chain managers, would possess the decryption keys specific to their roles. This way, they can unlock the encrypted information contained in the QR codes. Those without the necessary permissions wouldn't be able to decrypt the codes, ensuring the confidentiality of the product information remains intact.

(i) setup

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

During this phase, the trusted party (authority) creates two sets of information: Public Parameters (pk) and Master Key (mk): These parameters are shared publicly with all users and are used for both encryption and decryption. mk is kept strictly confidential and known only to the authority. It is used to generate encryption and decryption keys for individual users.

(ii) Encryption

When encrypting data, the user chooses a list of attributes that determine who can access it (access policy). Then, the user utilizes Public Parameters (pk) to encrypt the data (C) using the chosen attributes A .

The ciphertext $C = E(drug\,data, \mathrm{A})$ (13)

4.3.3 Blockchain-based Data Transmission

Blockchain technology is used in the pharmaceutical supply chain to securely track the movement of drugs by recording transactions as blocks on the blockchain. This allows stakeholders to quickly verify the authenticity and origin of pharmaceutical products in real-time. The unchangeable nature of blockchain ensures the integrity of data and makes it resistant to tampering, making it easier to monitor and confirm the accuracy of transactions. Encrypted data can be securely shared among authorized members of the supply chain using techniques ABE, which helps maintain privacy and confidentiality while efficiently detecting counterfeit products.

4.3.4 Shamir's Secret Sharing

Shamir developed a system, where confidential information (decryption key) is split into fragments and every participant gets their unique fragment. In this case, no single person can reassemble the information by themselves, but a certain number of them are needed in order to do so. The pharmaceutical supply chain finds it very important because it is used to manage access to sensitive information necessary for detecting fake drugs.

Shamir's Secret Sharing enhances the security and privacy of information used in counterfeit detection by requiring the collaboration of multiple parties to decrypt data. In dealing with sensitive pharmaceutical data, this is especially important because unauthorized access could result in theft, counterfeiting, or tampering with drug information.

Consider if you want to share a secret S (decryption key), among n participants but in such a way that any number of them can collaborate to reconstruct the secret. Selecting a prime number larger than the total number of participants and greater than the secret is essential so that this number can serve as foundation for calculations needed within secure contexts. Such prime numbers help us determine finite fields where all mathematical operations happen in such a way that information leakage never occurs.

Algorithm 2: Shamir's Secret Sharing process

Choose a Prime Number p

Select a prime number p that is larger than the maximum possible value of the secret S . This prime number defines the finite field over which the computations will be performed.

Decide on a threshold value k that represents the minimum number of shares required to reconstruct the secret S . It should be less than or equal to the total number of shares distributed.

Random Polynomial Generation:

Generate a random polynomial $f(x)$ of degree $k-1$ with the constant term being the secret S .

The polynomial has the form:

$$f(x) = S + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \bmod p$$

where $a_1, a_2, \ldots, a_{k-1}$, a_2 are randomly chosen coefficients from the finite field Z_p .

Share Generation:

For each participant i calculate their share s_i by evaluating the polynomial $f(x)$ at the point i .

$$s_i = f(i) \bmod p$$

Each participant i receives their share s_i without knowing the polynomial or other participants' shares.

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

Reconstruction:
Reconstruct the Secret S :
Use Lagrange interpolation to interpolate the polynomial passing through k points (shares).
Lagrange interpolation provides the unique polynomial of degree $k-1$ that passes through c given points.
The Secret S is the constant term of the reconstructed polynomial.

3.3.5 Authenticity Verification
Multi-Party Computation (MPC) ensures that each party involved in the computation only knows the final result of the function and nothing else about the input data of the other parties. This is crucial where privacy and security are important, such as verifying the authenticity of drugs and protecting sensitive information.

Let n be the number of parties involved in the MPC protocol. Each party P_i holds the private input x_i which represent data related to the drug's composition, batch numbers, or distribution details. $f(x_1, x_2, \ldots x_n)$ represents the computation function for verifying drug authenticity, which all parties want to compute jointly. $Enc(x)$ and $Dec(y)$ denote the encryption and decryption functions, respectively.

Each party P_i encrypts their input x_i to get $Enc(x_i)$.

The parties engage in a protocol to compute $Enc(y) = Enc(f(x_1, x_2, \ldots x_n))$ directly on the encrypted inputs. This step ensures that the computation is carried out without revealing any party's private input.

The encrypted result $Enc(y)$ is collaboratively decrypted by the parties to reveal the outcome

y , ensuring that no single party can decrypt the result on their own. Secure decryption protocols ensure that this process does not compromise the confidentiality of the inputs.

Secure Function Evaluation (SFE):

Consider a generic function f that verifies drug authenticity based on a comparison with reference data ref_i . let $g(x_i, ref_i)$ be a function that compares each party's input x_i with its corresponding reference value ref_i .

$Enc(y)$ is computed as a combination of these comparisons under encryption, such as using XOR operation $\oplus$ to derive the final decision on the drug's authenticity.

$$Enc(y) = Enc(f(x_1, x_2, \ldots x_n)) = \oplus_{i=1}^{n} Enc(g(x_i, ref_i)) \quad (14)$$

If the XOR operation yields a "1" (indicating a match) for all parties, the final $Enc(y)$ confirms authenticity. Conversely, any "0" (indicating a mismatch) raises flags regarding potential authenticity issues.

4.3.6 Decryption
When a user wants to decrypt the ciphertext C , they create a secret key (sk) based on their attributes. If the user's attributes match the access policy attached to the ciphertext, they can use their secret key to decrypt the ciphertext and retrieve the original plaintext data.

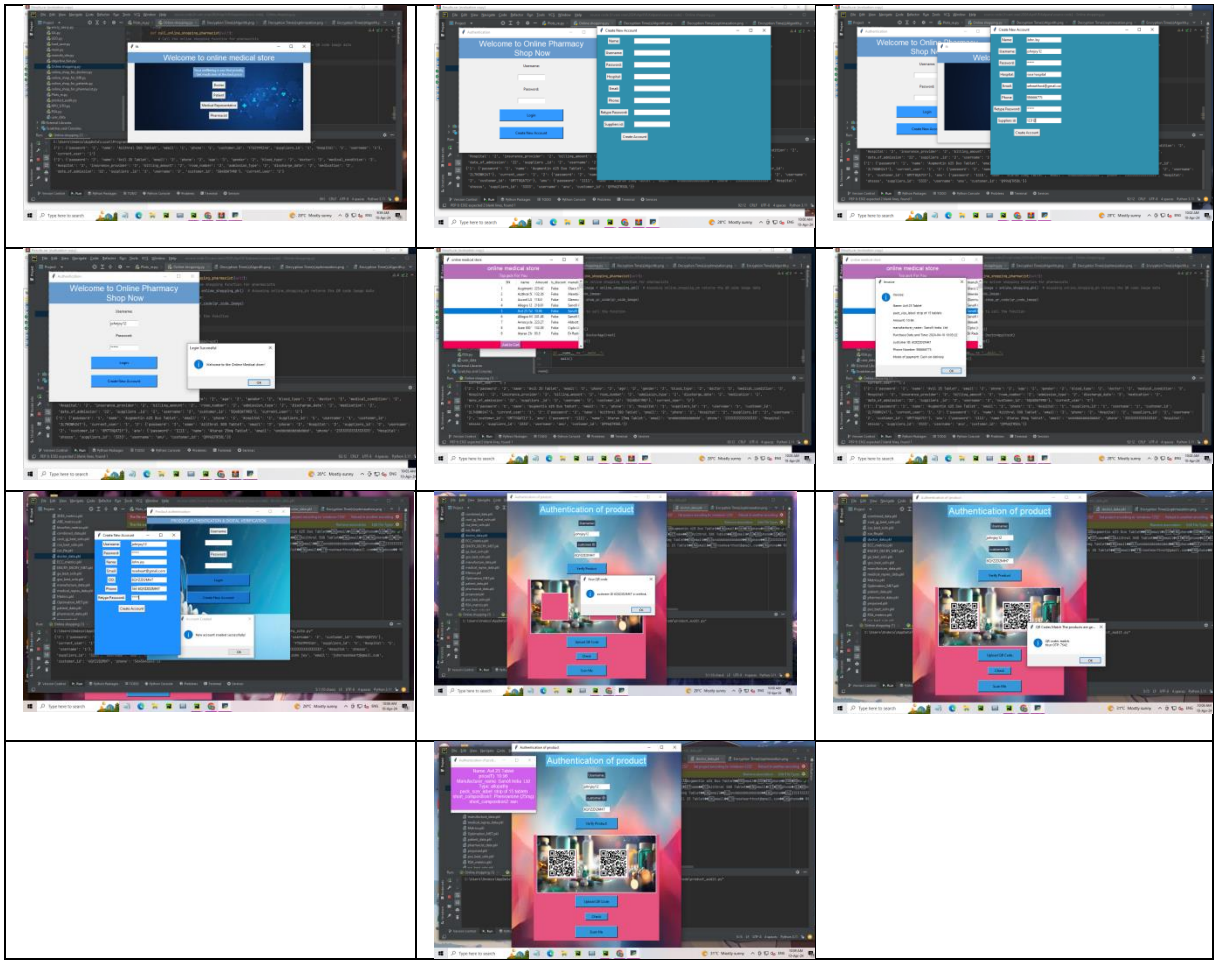
5. Experimental Results

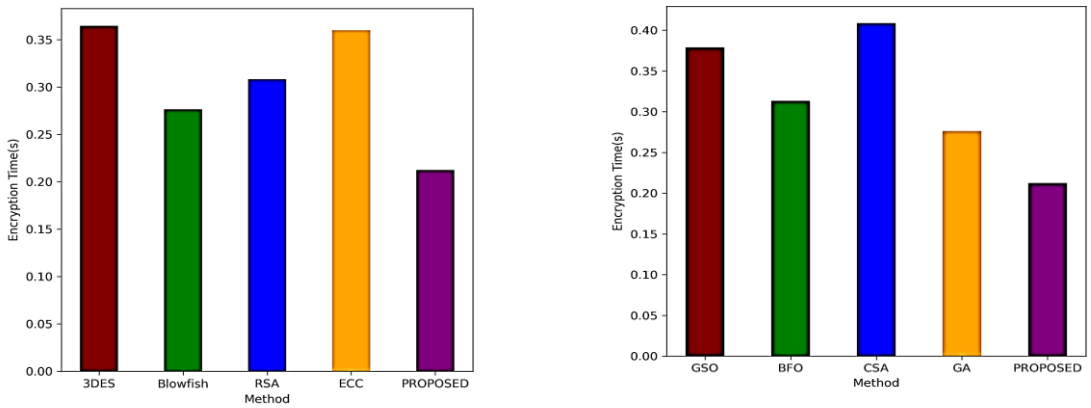
The proposed method is implemented using Python platform. We conducted cryptographic simulations and experiments using a high-performance hardware configuration, which included an Intel Core i7 processor with 8 cores, 16 GB DDR4 RAM, and a 500 GB SSD. To further boost computational power, we also utilized a NVIDIA

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

GeForce GTX 1660 Ti graphics card in our setup. For performance comparison, we considered several metrics such as encryption time, decryption time, turnaround time, and restoration efficiency. These metrics were measured for different encryption algorithms (3DES, Blowfish, RSA, ECC) and optimization algorithms (GSO, BFO, CSA, GA), along with our proposed hybrid algorithm.

Table 1: Simulation results





(a) **(b)**

Figure 4. Encryption time analysis (a) with Encryption algorithms (b) with optimization algorithms

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

The comparison of encryption speed, as shown in Figure 4, highlights significant differences in performance between traditional encryption methods and optimized techniques. In contrast to standard encryption methods such as 3DES, Blowfish, RSA, and ECC, the proposed algorithm stands out with an encryption time of 0.21234 seconds, which is notably faster than the others. Specifically, 3DES takes 0.36462 seconds, Blowfish takes 0.27655 seconds, RSA takes 0.308372 seconds, and ECC takes 0.35987 seconds. This signifies a substantial enhancement in speed.

Also, the proposed method outperforms other optimization algorithms like GSO, BFO, CSA, and GA when it comes to encryption time. The encryption time for the proposed method is the shortest at 0.21234 seconds. In comparison, GA takes longer with an encryption time of 0.2763 seconds, while GSO, BFO, and CSA have even slower times at 0.37904 seconds, 0.3134 seconds, and 0.40872 seconds respectively.

Figure 5 shows a thorough analysis of decryption times, comparing the proposed method to traditional encryption algorithms and current optimization techniques. The proposed method outperforms 3DES, Blowfish, RSA, and ECC with a decryption time of 0.22112 seconds, demonstrating superior speed and efficiency in decoding encrypted data. The performance of the proposed method is significantly better than 3DES (0.33442 seconds), Blowfish (0.2565 seconds), RSA (0.312773 seconds), and ECC (0.321232 seconds).

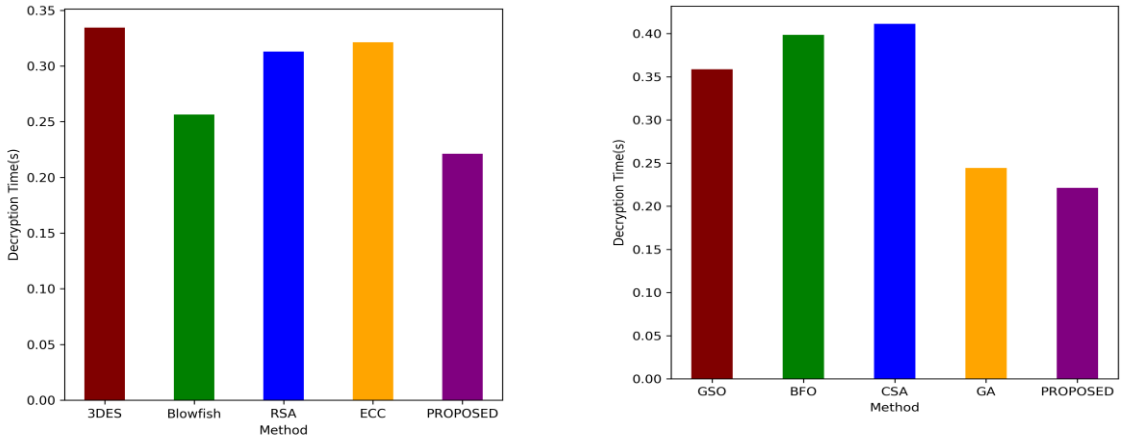
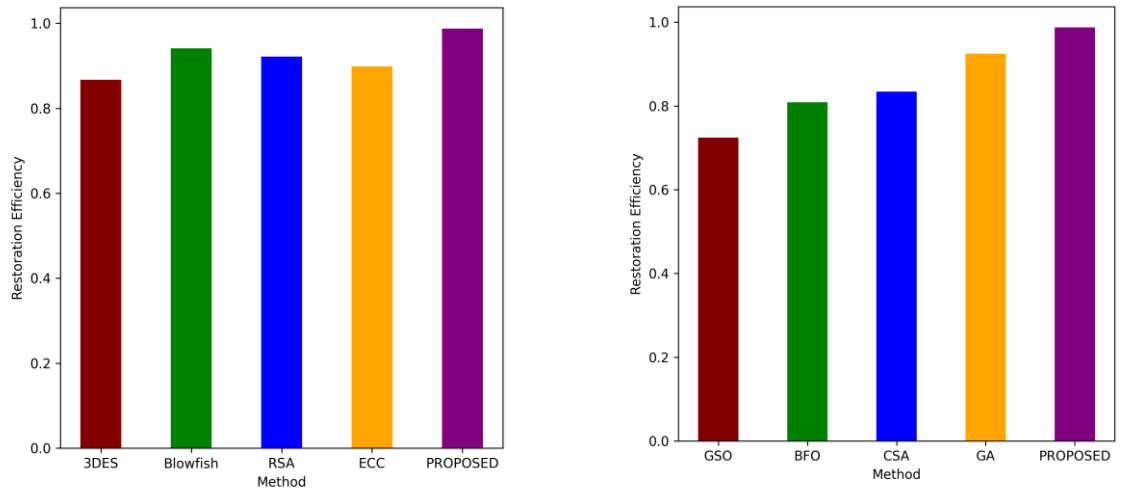


Figure 5. Decryption time analysis (a) with Encryption algorithms (b) with optimization algorithms

When compared to other optimization algorithms like GSO, BFO, CSA, and GA, the proposed method proves its effectiveness by achieving the fastest decryption time of 0.22112 seconds. This is a significant improvement over the decryption times of GSO (0.35864 seconds), BFO (0.39865 seconds), CSA (0.41131 seconds), and GA (0.24432 seconds).

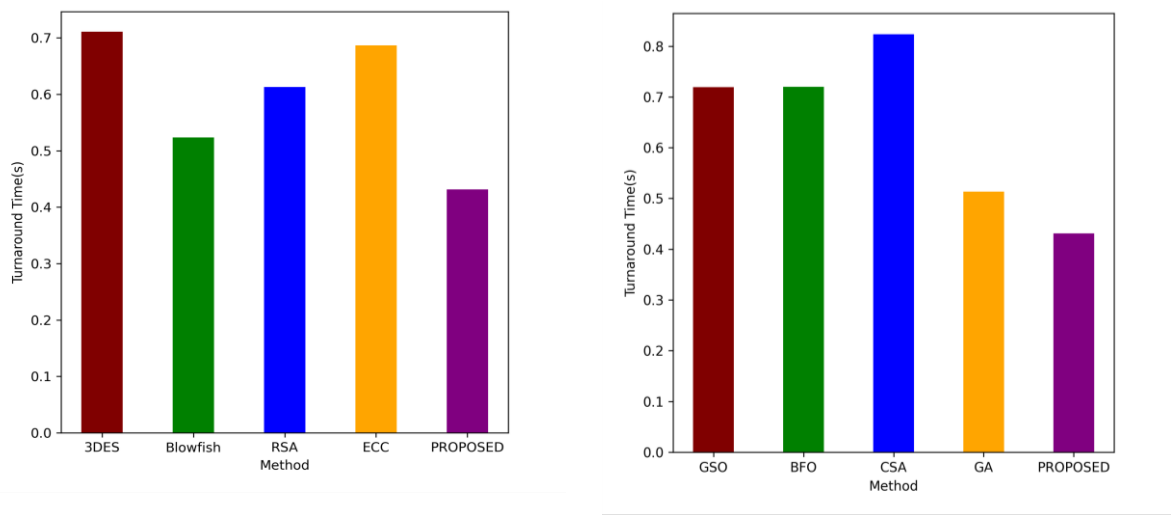
DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024



(a) **(b)**

Figure 6: Restoration efficiency comparison (a) with Encryption algorithms (b) with optimization algorithms

The analysis in Figure 6 examines how well data integrity is maintained after decryption. It compares traditional encryption methods like 3DES, Blowfish, RSA, and ECC with newer optimization algorithms like GSO, BFO, CSA, and GA. The proposed method has shown to be more effective in preserving data integrity post-decryption, with a restoration efficiency score of 0.987453. This score surpasses the performance of 3DES, Blowfish, RSA, and ECC. In the same way, when looking at optimization algorithms, the proposed method once again shows exceptional performance, outperforming GSO, BFO, CSA, and GA.



(a) **(b)**

Figure 7: Turnaround Time analysis (a) with Encryption techniques (b) with optimization algorithms

In Figure 7fta, we compare the turnaround time of various encryption algorithms, considering both encryption and decryption times to evaluate their overall performance. This metric is important for evaluating how quickly and efficiently data processing systems operate. (a) The proposed encryption method has a turnaround time of 0.431231 seconds, which is notably quicker than 3DES at 0.710983 seconds, Blowfish at 0.52356 seconds, RSA at 0.612883 seconds, and ECC at 0.68672 seconds. Similarly, compared to other optimization algorithms, the this method excels with a fast turnaround time of 0.431231 seconds, outrunning GSO at 0.71954 seconds, BFO at 0.71978 seconds, CSA at 0.823451 seconds, and GA at 0.51345 seconds. Both Table 2 and Table 3 provide the numerical values obtained for all the methods.

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

Table 2: Comparative Analysis with existing Encryption algorithms

Metrics/Methods	3DES	Blowfish	RSA	ECC	PROPOSED
Encryption Time(s)	0.36462	0.27655	0.308372	0.35987	0.21234
Decryption Time(s)	0.33442	0.2565	0.312773	0.321232	0.22112
Turnaround Time(s)	0.710983	0.52356	0.612883	0.68672	0.431231
Restoration Efficiency	0.867372	0.94109	0.92133	0.898773	0.987453

Table 3: Comparative Analysis with Existing Optimization algorithms

Metrics/Methods	GSO	BFO	CSA	GA	PROPOSED
Encryption Time(s)	0.37904	0.3134	0.40872	0.2763	0.21234
Decryption Time(s)	0.35864	0.39865	0.41131	0.24432	0.22112
Turnaround Time(s)	0.71954	0.71978	0.823451	0.51345	0.431231
Restoration Efficiency	0.72433	0.808432	0.83432	0.92453	0.987453

6. Conclusions

The new hybrid optimization algorithm described in this article showed better performance in encryption and decryption speed, turnaround time, and restoration effectiveness compared to current methods. By using a group teaching strategy based on educational techniques, the encryption key selection was improved, resulting in a more secure system overall. Furthermore, including Shamir's Secret Sharing in the process ensures safe sharing of decryption keys among authorized users, effectively guarding against unauthorized access to sensitive information and enhancing security against counterfeit detection. The proposed algorithm was able to encrypt data in just 0.21234 seconds, which is faster than Blowfish's encryption time of 0.27655 seconds. Additionally, the decryption time of 0.22112 seconds and overall processing time of 0.431231 seconds for the new algorithm outperformed the other algorithms in comparison. In the future, we could explore how well the algorithm can be used in distributed systems, improve its ability to withstand attacks from adversaries and threats from quantum computing.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Uddin M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. International Journal of Pharmaceutics. 2021 Mar 15; 597:120235.

[2] Panda SK, Satapathy SC. Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. Personal and Ubiquitous Computing. 2021 Jul 29:1-7.

[3] Suresh Kumar K, Nassa VK, Uike D, Sahu AK, Athavale VA, Saravanan V. A Comparative Analysis of Blockchain in Enhancing the Drug Traceability in Edible Foods Using Multiple Regression Analysis. Journal of Food Quality. 2022 Jun 23; 2022.

[4] Leal F, Chis AE, Caton S, González–Vélez H, García–Gómez JM, Durá M, Sánchez–García A, Sáez C, Karageorgos A, Gerogiannis VC, Xenakis A. Smart pharmaceutical manufacturing: Ensuring end-to-end traceability and data integrity in medicine production. Big Data Research. 2021 May 15; 24:100172.

[5] Akhtar MM, Rizvi DR. Traceability and detection of counterfeit medicines in pharmaceutical supply chain using blockchain-based architectures. Sustainable and energy efficient computing paradigms for society. 2021:1-31.

[6] Nitsche B, Straube F, Kämper TL, Zarnitz S. Implementation framework for blockchain-based traceability to tackle drug-counterfeiting: embracing sustainable pharma logistics networks. InGlobal Conference on Sustainable Manufacturing 2022 Oct 5 (pp. 630-637). Cham: Springer International Publishing.

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

[7] Lau WF, Liu DY, Au MH. Blockchain-based supply chain system for traceability, regulation and anti-counterfeiting. In2021 IEEE International Conference on Blockchain (Blockchain) 2021 Dec 6 (pp. 82-89). IEEE.

[8] Bandhu KC, Litoriya R, Lowanshi P, Jindal M, Chouhan L, and Jain S. Making drug supply chain secure traceable and efficient: a Blockchain and smart contract based implementation. Multimedia Tools and Applications. 2023 Jun; 82(15):23541-68.

[9] Raijada D, Wac K, Greisen E, Rantanen J, Genina N. Integration of personalized drug delivery systems into digital health. Advanced drug delivery reviews. 2021 Sep 1; 176:113857.

[10] Haji M, Kerbache L, Al-Ansari T. Food quality, drug safety, and increasing public health measures in supply chain management. Processes. 2022 Aug 28; 10(9):1715.

[11] Tahmasbzadeh A, Kabirirad S. A Blockchain-Based Approach for Data Storage in Drug Supply Chain. In2023 9th International Conference on Web Research (ICWR) 2023 May 3 (pp. 335-341). IEEE.

[12] Ma JY, Shi L, Kang TW. The effect of digital transformation on the pharmaceutical sustainable supply chain performance: The mediating role of information sharing and traceability using structural equation modeling. Sustainability. 2022 Dec 30; 15(1):649.

[13] Gayialis SP, Kechagias EP, Papadopoulos GA, Masouras D. A review and classification framework of traceability approaches for identifying product supply chain counterfeiting. Sustainability. 2022 May 30; 14(11):6666.

[14] Liu S, Zhang R, Liu C, Shi D. P-PBFT: An improved blockchain algorithm to support large-scale pharmaceutical traceability. Computers in biology and medicine. 2023 Mar 1; 154:106590.

[15] Dasaklis TK, Voutsinas TG, Tsoulfas GT, Casino F. A systematic literature review of blockchain-enabled supply chain traceability implementations. Sustainability. 2022 Feb 20; 14(4):2439.

[16] Li J, Han D, Wu Z, Wang J, Li KC, Castiglione A. A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control. Future Generation Computer Systems. 2023 May 1; 142:195-211.

[17] Li L, Qu H, Wang H, Wang J, Wang B, Wang W, Xu J, Wang Z. A Blockchain-Based Product Traceability System with Off-Chain EPCIS and IoT Device Authentication. Sensors. 2022 Nov 10;22(22):8680.

[18] Bapatla AK, Mohanty SP, Kougianos E. PharmaChain 3.0: Efficient Tracking and Tracing of Drugs in Pharmaceutical Supply Chain Using Blockchain Integrated Product Serialization Mechanism. SN Computer Science. 2024 Jan 5; 5(1):149.

[19] Durá M, Leal F, Sánchez-García Á, Sáez C, García-Gómez JM, Chis AE, González-Vélez H. Blockchain for data originality in pharma manufacturing. Journal of Pharmaceutical Innovation. 2023 Jul 7:1-9.

[20] Sabah S, Hasan AT, Daria A. A blockchain-based approach to detect counterfeit drugs in medical supply chain. InProceedings of the International Conference on Big Data, IoT, and Machine Learning: BIM 2021 2021 Dec 4 (pp. 609-621). Singapore: Springer Singapore.

[21] Musamih A, Salah K, Jayaraman R, Arshad J, Debe M, Al-Hammadi Y, Ellahham S. A blockchain-based approach for drug traceability in healthcare supply chain. IEEE access. 2021 Jan 8; 9:9728-43.

[22] Turki M, Cheikhrouhou S, Dammak B, Baklouti M, and Mars R, Dhahbi A. NFT-IoT pharma chain: IoT drug traceability system based on blockchain and non-fungible tokens (NFTs). Journal of King Saud University-Computer and Information Sciences. 2023 Feb 1; 35(2):527-43.

[23] Tan X, Kang Z, Wei F, Gao C, Wei Z, Huang H. MB-BC: drug traceability system based on multibranched blockchain structure. Wireless Communications and Mobile Computing. 2022 Jul 25; 2022:1-4.

[24] Nawaz A, Wang L, Irfan M, Westerlund T. Hyperledger sawtooth based supplychain traceability system for counterfeit drugs. Computers & Industrial Engineering. 2024 Feb 27:110021.

[25] Rai BK. BBTCD: blockchain based traceability of counterfeited drugs. Health Services and Outcomes Research Methodology. 2023 Sep; 23(3):337-53.

[26] Bandhu KC, Litoriya R, Lowanshi P, Jindal M, Chouhan L, and Jain S. Making drug supply chain secure traceable and efficient: a Blockchain and smart contract based implementation. Multimedia Tools and Applications. 2023 Jun; 82(15):23541-68.

[27] Reem Atassi , Fuad Alhosban, Fusion Optimization and Classification Model for Blockchain Assisted Healthcare Environment, Fusion: Practice and Applications, Vol. 9 , No. 2 , (2022) : 62-73 (Doi : https://doi.org/10.54216/FPA.090205)

[28] Lisha Yugal, Suresh Kaswan, B. S. Bhatia, Aditi Sharma, IoT-based Emulated Performance Evaluation NLP Model for Advanced Learners in Academia 4.0 and Industries 4.0, Journal of Intelligent Systems and Internet of Things, Vol. 10 , No. 2 , (2023) : 36-75 (Doi : https://doi.org/10.54216/JISIoT.100206)

[29] Shereen Zaki,Mahmoud M. Ibrahim,Mahmoud M. Ismail, Interval Valued Neutrosophic VIKOR Method for Assessment Green Suppliers in Supply Chain, Journal of International Journal of Advances in Applied

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024

Computational Intelligence, Vol. 2 , No. 1 , (2022) : 15-22 (Doi : https://doi.org/10.54216/IJAACI.020102)

DOI: https://doi.org/10.54216/FPA.170206
Received: January 21, 2024 Revised: April 14, 2024 Accepted: September 18, 2024