American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Anonymous Whistleblower Protection Platform with Secure Evidence Submission for E-Commerce

Jawaji Samyuktha, G. Arpitha*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: G. Arpitha

ABSTRACT

Business organizations have huge potential to increase their customer base by offering e-commerce services, especially in the post-pandemic era. Ensuring secure e-commerce applications plays an important role in increasing the customer base. To develop appropriate policies and secure technological infrastructures, business organizations first need to establish an understanding of the reservations of their customers toward e-commerce, as well as their perception of security and privacy of e-commerce applications. This research presents a Flask web application designed to ensure confidentiality, integrity, and accountability in digital marketplaces. The system enables secure user authentication with role-based access control for Admin, Seller, and Customer roles, ensuring controlled access to platform functionalities. Sensitive files and confidential messages are encrypted using a 16-round Feistel cipher (FC) before storage, protecting data from unauthorized access or tampering. Encrypted files are securely stored in the server directory, while metadata, user information, encryption keys, and audit logs are maintained in Tiny Database (TinyDB). The platform also includes encryption key rotation, secure file decryption upon authorization, and detailed audit logging for traceability of system activities. By integrating encryption mechanisms, session security, and structured access control within a unified web framework, the proposed system enhances digital trust, supports ethical reporting, and strengthens governance in modern e-commerce environments.

1. INTRODUCTION

E-commerce is the use of computing devices and communication platforms to conduct business online. It has proven to be an important enabler for business organizations by expanding their reach to global customers, cost-effectively and efficiently. This technological revolution is termed disruptive technology as it has changed traditional business models and brought about new business approaches. This extensive digital transformation process requires changes in organizational processes, human resources, and technological infrastructure. To be successful, business organizations need to carry out a detailed analysis of their marketplace to develop an effective business strategy, which requires financial and human resources. Furthermore, e-commerce adoption is also dependent on social, legal, economic, political, and technological factors. The difference in technology accessibility, level of skills, security concerns, shopping behavior, purchasing power, cultural differences, and legislation also affect the acceptance of e-commerce. As a result, the adoption of technological infrastructure by business organizations varies considerably across the globe. The rapid advancement of information technology has significantly transformed the landscape of commerce, leading to a proliferation of non-face-to-face e-commerce services worldwide. Personal identity proofing (PIP) has become essential for verifying users' identities in online transactions such as payments, refunds, membership registrations, and access to age-restricted products. Traditionally, personal identifiable information (PII) provided by credible third parties such as social security numbers, driver's licenses, and passports has been used to identify individuals. However, the online environment presents unique challenges in protecting user privacy while ensuring secure authentication.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Despite the development of various PIP methods, including knowledge-based authentication, biometric verification, and digital certificates, existing systems often face issues related to privacy concerns, user convenience, and security vulnerabilities. The indiscriminate collection and use of sensitive personal information have led to social problems such as identity theft and infringement on individual privacy. In some cases, the misuse of unchangeable personal identifiers exacerbates these issues. There is a pressing need for improved PIP methods that balance security, privacy, and user convenience, while empowering users with control over their personal information.

2. LITERATURE SURVEY

Akram, et al. [1] highlighted that the adoption of mobile commerce increased significantly during the COVID-19 pandemic due to factors such as ease of use, mobility, customer engagement, and trust in digital platforms. The study emphasized that consumers increasingly preferred smartphones for shopping because they provided convenient access to products and services from any location. Secure payment methods, user-friendly interfaces, and personalized shopping experiences further enhanced customer satisfaction and encouraged continuous use of mobile commerce applications. Gu, et al. [2] examined the impact of the COVID-19 pandemic on consumer buying behavior and observed that customers became more familiar with online shopping platforms, resulting in long-term changes in purchasing habits. The study reported that consumers developed greater confidence in digital transactions and increasingly relied on e-commerce platforms for both essential and non-essential products. Guthrie, et al. [3] investigated changes in consumer purchase intentions during the pandemic and found a significant shift toward purchasing essential goods while reducing expenditure on luxury products. The study also highlighted the growing preference for contactless shopping and home delivery services, demonstrating how the pandemic accelerated digital transformation within the retail sector. Shu and Liu [4] focused on the security challenges accompanying the rapid expansion of e-commerce and emphasized that although organizations have implemented several cybersecurity mechanisms, advanced privacy-enhancing technologies and stronger security strategies are still required to protect customer information and improve confidence in online transactions. Mohammed, et al. [5] identified online safety perception, privacy concerns, personal preferences, and acceptance of digital technologies as the major factors influencing consumer adoption of e-commerce platforms, concluding that secure and transparent systems significantly improve customer willingness to engage in online shopping.

Clemons, et al. [6] examined the influence of organizational reputation on customer trust and found that consumers often evaluate the credibility of e-commerce platforms based on reputation, previous customer experiences, and public perception. The study also observed that the impact of organizational reputation differs across geographical regions due to cultural and economic variations, emphasizing the importance of region-specific trust-building strategies. López Jiménez, et al. [7] demonstrated that displaying recognized security seals and certifications on commercial websites significantly improves customer confidence by assuring users about transaction security and data protection. The implementation of these trust indicators resulted in increased website traffic, higher conversion rates, and improved online sales performance. Dhende and Meshram [8] investigated the security challenges associated with information exchange among customers, organizations, suppliers, and business partners through advanced technological infrastructures. The study highlighted risks such as unauthorized access, information leakage, and cyberattacks, emphasizing the need for robust

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

security frameworks and secure communication mechanisms. Tan [9] reported that lack of customer trust continues to be one of the major obstacles to the widespread adoption of electronic commerce despite technological advancements. The study emphasized that building customer trust requires consistent service quality, transparent business practices, and reliable security measures, while rebuilding trust after security incidents is considerably more difficult and expensive. Zhang, et al. [10] further explained that restoring customer trust requires an integrated strategy combining immediate transactional recovery with long-term relationship-building approaches, including transparent communication, effective customer support, and continuous security improvements.

Turner, et al. [11] investigated how users with limited technical knowledge evaluate the security of online shopping platforms and found that they primarily depend on website reputation, previous experiences, visible security indicators, and recommendations from trusted third parties when deciding whether to conduct online transactions. The study emphasized the importance of providing clear security information and designing user-friendly websites to improve customer confidence. Liebermann and Stashevsky [12] examined the influence of demographic characteristics and user behavior on perceived internet risks and developed a comprehensive risk perception model that helps users better understand potential online security threats. The research highlighted that increasing user awareness through education and training can significantly improve secure online behavior. Belanger, et al. [13] emphasized that customer perception of a merchant's trustworthiness is one of the most important factors influencing both online and traditional purchasing decisions. The study concluded that security, privacy protection, website usability, and transparent business practices collectively encourage stronger purchase intentions and greater customer confidence. Yenisey, et al. [14] conducted experimental research using simulated e-commerce applications to identify the factors that promote positive customer experiences during online shopping. The study found that intuitive website navigation, transparent transaction processes, effective security features, and consistent system performance significantly improve customer trust, increase user satisfaction, and encourage continued participation in electronic commerce platforms.

3. PROPOSED SYSTEM

The research as shown in Fig. 1 is a secure, role-based whistleblower protection platform designed for e-commerce environments that ensures confidential evidence submission and protected communication. It integrates file encryption, encrypted messaging, access control mechanisms, and audit logging to safeguard sensitive data. By implementing encryption using a Feistel-based cipher and structured user roles (Admin, Seller, Customer), the system enhances data privacy, prevents unauthorized access, and strengthens digital accountability within the platform.

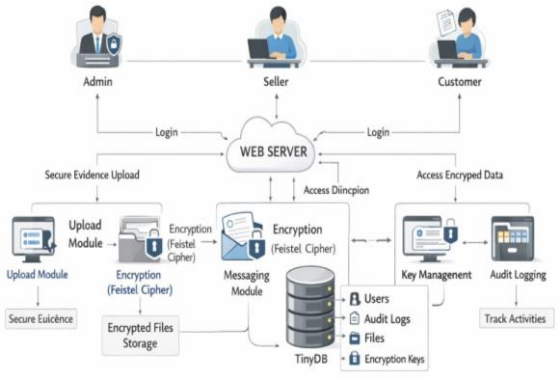

Fig. 1: Proposed system architecture

1. User Registration and Authentication: Users register by selecting their role and providing required credentials. Passwords are securely hashed before storage to ensure protection against credential theft. Upon successful login, session-based authentication grants role-specific dashboard access.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

2. Secure Evidence Upload by Seller: The seller uploads evidence files through the secure upload module. Before storage, the file is encrypted using a FC with an active encryption key. Only the encrypted file is stored in the system, ensuring data confidentiality at rest.

3. Metadata Storage and Access Control: File metadata such as uploader ID, target customer, and timestamps are stored in the database. Role-based access control verifies who can access, decrypt, or download the file. Unauthorized users are automatically restricted from viewing sensitive content.

4. Secure Encrypted Communication: Users can send messages within the system, with an option to encrypt confidential messages. Encrypted messages are stored in encoded format and can only be decrypted by authorized participants. This ensures protected internal communication.

5. Controlled Decryption and Download: Authorized users can request file decryption through the platform. The system retrieves the encrypted file, applies decryption using the active key, and provides secure access. All such actions are logged for accountability.

6. Audit Logging and Monitoring: Every critical activity, including login, upload, download, decryption, and key updates, is recorded in audit logs. The administrator can monitor system activities to ensure transparency and detect misuse. This strengthens governance and digital trust.

3.1 FC encryption

FC is a symmetric key cryptographic structure used to build secure block ciphers, as illustrated in Fig. 2. It divides input data into two halves and processes them through multiple rounds of substitution and permutation using a secret key. The same structure is used for both encryption and decryption, making it computationally efficient. In this project, the FC is used to encrypt uploaded files and confidential messages to ensure data confidentiality and secure storage.

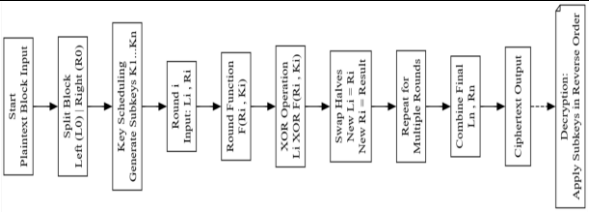

Fig. 2: Internal workflow of FC encryption

1. Plaintext Block Preparation: The input plaintext is first converted into binary format if necessary. The data is divided into fixed-size blocks depending on the cipher configuration. Each block is processed independently to ensure structured encryption.

2. Splitting into Two Halves: Each block is divided into two equal parts: Left Half (L0) and Right Half (R0). These halves act as inputs for the first round of encryption. This split enables iterative transformation using the Feistel structure.

3. Key Scheduling and Subkey Generation: The main secret encryption key is processed through a key scheduling algorithm. This generates multiple round-specific subkeys (K1, K2, K3, … Kn). Each round uses a different subkey to enhance security.

4. Round Function Input Processing: The Right half (Ri) is passed into a round function F along with the corresponding subkey Ki. This function may include operations like substitution, permutation, expansion, or bitwise mixing. The purpose is to create a complex transformation of the input.

5. XOR Operation with Left Half: The output of the round function F(Ri, Ki) is XORed with the Left half (Li). This operation mixes the data from both halves, introducing confusion and diffusion. The result becomes the new Right half for the next stage.

6. Swapping of Halves: After the XOR operation, the original Right half becomes the new Left half. The modified result becomes the new Right half. This swapping mechanism ensures proper data propagation across rounds.

7. Iterative Round Execution: Steps 4, 5, and 6 are repeated for multiple rounds. Each round increases encryption strength by further

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

scrambling the data. The security of the cipher largely depends on the number of rounds used.

8. Final Combination of Halves: After completing all rounds, the final Left and Right halves are combined. Depending on implementation, a final swap may or may not occur. The merged output forms the ciphertext block.

9. Ciphertext Output Generation: All encrypted blocks are combined to produce the complete ciphertext. This encrypted data is then stored or transmitted securely. The ciphertext appears random and unintelligible without the key.

10. Decryption Using Reverse Subkeys: For decryption, the same Feistel structure is used. The only difference is that subkeys are applied in reverse order (Kn to K1). This reversibility makes FCs efficient and symmetric in design.

4. RESULTS AND DESCRIPTION

The Fig. 3 shows output represents the Product Management page after a seller successfully uploads a product. A confirmation message "Product added successfully!" appears at the top, indicating successful database insertion. The seller can add new products using the form fields such as Product Name, Description, Price, and Category. On the right side, the "My Products" section shows the newly added product (iPhone) with its category, price, status marked as active, and an option to delete, confirming that the product has been successfully stored and is now available in the system.

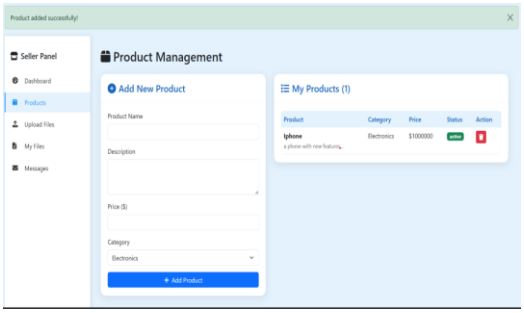

Fig. 3: Product uploaded by seller

The Fig. 4 shows displayed output that represents the Secure File Upload page after a seller successfully uploads and encrypts a file. A confirmation message "File uploaded and encrypted successfully!" appears at the top, indicating that the file has been encrypted using the FC and securely stored. The interface provides a drag-and-drop upload area along with fields for file description and optional target customer selection. On the right side, the Encryption Info panel highlights that a 16-round FC is used, including secure key derivation, block cipher mode, and padding support, confirming that the file is protected before storage.

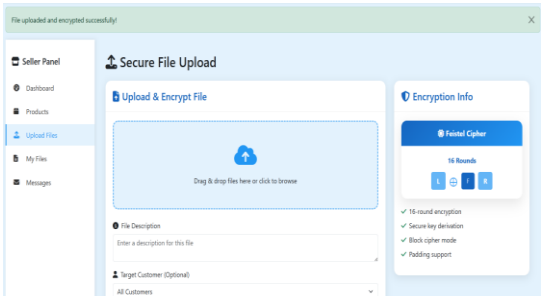

Fig. 4: File uploaded by seller

The Fig. 5 represents the updated Customer Dashboard of the Secure Commerce platform. The customer can navigate through options such as Dashboard, Browse Products, Download Files, Decrypt Files, and Messages from the left panel. In the main section, the customer is viewing available products under the "Browse Products" page, where the listed item (iPhone) shows its category, price, description, and seller information. This interface allows customers to explore active products, access encrypted files if permitted, and interact securely within the system.

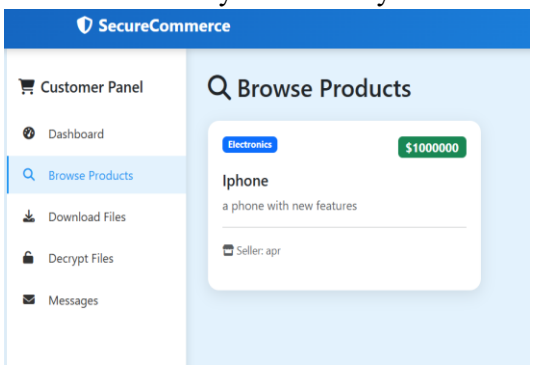

Fig. 5: Customer dashboard updated after product uploading

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

The Fig. 6 represents the Download Encrypted Files page in the Customer Panel of the Secure Commerce platform. It shows a list of available encrypted files along with details such as file name, description, uploader, upload date, and encryption status. Each file provides two download options: Encrypted Download, which allows the customer to download the file in its secured encrypted form, and Decrypted Download, which automatically decrypts the file before downloading in its original format. This interface ensures secure file distribution while maintaining controlled access and encryption integrity.

Fig. 6: Files downloading interface

The Fig. 7 represents the File Decryption Interface in the Customer Panel after a successful decryption operation. The customer selects an encrypted file from the dropdown menu and initiates the decryption process using the "Decrypt File" button. A confirmation message "Decryption Successful!" appears, indicating that the selected file has been securely decrypted using the FC. The interface then provides a "Download Decrypted File" option, allowing the customer to download the file in its original readable format while maintaining controlled and authorized access.

Fig. 7: Decrypted selected file

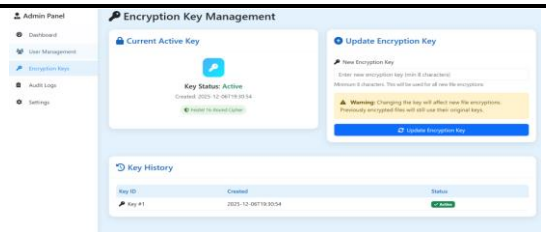

Fig. 8: Encryption key management interface

The Fig. 8 represents the Encryption Key Management page in the Admin Panel of the Secure Commerce platform. It shows the currently active encryption key status, including its creation date and confirmation that the system is using a 16-round FC. The admin is provided with an option to update the encryption key by entering a new key with a minimum length requirement, along with a warning that key changes will affect only new file encryptions. The page also includes a Key History section displaying previously generated keys and their status, ensuring secure key rotation, traceability, and centralized encryption control.

5. CONCLUSION

This research successfully addresses the critical need for confidentiality, integrity, and accountability in digital marketplaces by integrating role-based access control, encrypted file storage, secure messaging, and centralized audit logging within a unified Flask-based system. The platform ensures that sensitive evidence is encrypted using a 16-round FC before storage, preventing unauthorized access and protecting whistleblower data from exposure or tampering. Through structured user roles (Admin, Seller, and Customer), the system enforces strict permission validation, allowing controlled file access, secure decryption, and monitored communication between participants. The inclusion of encryption key management with rotation capability enhances long-term cryptographic security, while detailed audit logs strengthen transparency and traceability of all critical operations such as login, upload, decryption, and key updates. By combining secure authentication, encrypted storage, protected

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

messaging, and administrative oversight, the project establishes a robust and scalable security framework suitable for modern e-commerce environments, promoting ethical reporting, digital trust, and improved governance within online platforms.

REFERENCES

[1]. Akram, U.; Fülöp, M.T.; Tiron-Tudor, A.; Topor, D.I.; Căpușneanu, S. Impact of Digitalization on Customers' Well-Being in the Pandemic Period: Challenges and Opportunities for the Retail Industry. Int. J. Environ. Res. Public Health **2021**, 18, 7533.

[2]. Gu, S.; Ślusarczyk, B.; Hajizada, S.; Kovalyova, I.; Sakhbieva, A. Impact of the COVID-19 Pandemic on Online Consumer Purchasing Behavior. J. Theor. Appl. Electron. Commer. Res. **2021**, 16, 2263–2281.

[3]. Guthrie, C.; Fosso-Wamba, S.; Arnaud, J.B. Online consumer resilience during a pandemic: An exploratory study of e-commerce behavior before, during and after a COVID-19 lockdown. J. Retail. Consum. Serv. **2021**, 61, 102570.

[4]. Shu, S.; Liu, Y. Looking Back to Move Forward: A Bibliometric Analysis of Consumer Privacy Research. J. Theor. Appl. Electron. Commer. Res. **2021**, 16, 727–747.

[5]. Mohammed, Z.A.; Tejay, G.P. Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. Comput. Secur. 2017, 67, 254–265.

[6]. Clemons, E.K.; Wilson, J.; Matt, C.; Hess, T.; Ren, F.; Jin, F.; Koh, N.S. Global Differences in Online Shopping Behavior: Understanding Factors Leading to Trust. J. Manag. Inf. Syst. 2016, 33, 1117–1148.

[7]. Jiménez, D.L.; Dittmar, E.; Portillo, J.V. The Use of Trust Seals in European and Latin American Commercial Transactions. J. Open Innov. Technol. Mark. Complex. 2021, 7, 150.

[8]. Dhende, K.; Meshram, S. Review of e-Commerce Security Challenges. Turk. J. Comput. Mathe-Matics Educ. (TURCOMAT) 2021, 12, 3593–3598.

[9]. Tan, Y.C.L. Recent Technological Trends and Security Challenges in Trust-Building in E-Commerce. Int. J. Bus. Manag. 2021, 14, 226.

[10]. Zhang, H.D.; Chen, S.C.; Ruangkanjanases, A. Benefits First: Consumer Trust Repair in Mobile Commerce. J. Theor. Appl. Electron. Commer. Res. 2021, 16, 1079–1096.

[11]. Turner, C.W.; Zavod, M.; Yurcik, W. Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites. In Proceedings of the Fourth International Conference on Electronic Commerce Research, Dallas, TX, USA, 8–11 November 2021; pp. 628–636.

[12]. Liebermann, Y.; Stashevsky, S. Perceived risks as barriers to Internet and e-commerce usage. Qual. Mark. Res. Int. J. 2022, 5, 291–300.

[13]. Belanger, F.; Hiller, J.S.; Smith, W.J. Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. J. Strat. Inf. Syst. 2022, 11, 245–270.

[14]. Yenisey, M.M.; Ozok, A.; Salvendy, G. Perceived security determinants in e-commerce among Turkish university students. Behav. Inf. Technol. 2015, 24, 259–274.