The IJICS (International Journal of Informatics and Computer Science)
Vol 9 No 2, July 2025, Page 121-127
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

Web-Based E-Business Application with Customer Data Encryption Feature to Protect Privacy at CV Jasa Karya Rizki

Lola Kamal Siregar* , Ali Ikhwan

Information Systems, State Islamic University of North Sumatra, Medan, Indonesia
Email: [1]lolakamalsiregar01@gmail.com, [2]aliikhwan@uinsu.ac.id
(* lolakamalsiregar01@gmail.com)
Submitted: **22/07/2025**; Accepted: **30/07/2025**; Published: **31/07/2025**

Abstract− This research presents the development of a web-based e-business application integrated with a data encryption feature using the Data Encryption Standard (DES) algorithm to protect customer privacy. The system is designed for CV Jasa Karya Rizki to manage customer and transaction data securely. DES encryption is implemented manually using PHP without relying on external libraries. The encryption process is applied during data input to ensure that only ciphertext is stored in the database. When data needs to be accessed, decryption is performed on-the-fly, allowing authorized users to view the original information securely. The application consists of core modules for managing customer data, transactions, products, and reports. Encryption and decryption functions are encapsulated within the system's main classes, enhancing maintainability and modularity. Testing results show that the DES implementation functions correctly, providing a secure data management workflow without negatively impacting system performance. This research demonstrates that classic encryption algorithms like DES can still be effectively applied in small-scale business environments to enhance data security and customer trust.

Keywords: E-Business, Data Encryption, Des Algorithm, Data Security, Web Application.

1. INTRODUCTION

The advancement of digital technology has brought about transformative changes in how businesses operate, interact with customers, and manage their internal processes. In recent years, the integration of technology into almost every business sector has become a necessity rather than an option [1]. One of the most significant advancements is the emergence of e-business systems, which allow companies to conduct transactions, store and process customer data, and expand their market reach without the limitations of physical boundaries [2][3]. The adoption of such systems has been driven by the need for efficiency, accessibility, and competitive advantage in the fast-paced global market [4][5].

E-business platforms, particularly those that are web-based, offer a range of benefits including faster transaction processing, 24/7 availability, and cost reduction in operational activities [6][7]. Businesses can connect with customers in real time, automate repetitive tasks, and gain valuable insights from data analytics embedded in these systems. However, the reliance on digital platforms also exposes businesses to new types of risks, especially related to the security and privacy of stored information [8][9]. Customer data—such as names, addresses, contact numbers, and transaction histories—can be a prime target for cybercriminals aiming to exploit or sell such information for illicit purposes.

Data breaches and cyberattacks have become increasingly common, and the consequences can be devastating for businesses [10][11]. A single security incident can lead to financial losses, loss of customer trust, and even legal penalties due to non-compliance with data protection regulations. In the digital economy, where trust plays a critical role in customer relationships, protecting sensitive information is no longer optional—it is a fundamental requirement for long-term business sustainability. This makes the integration of data protection mechanisms into e-business platforms not just advisable, but imperative.

One of the most reliable and widely used approaches to securing digital information is data encryption. Encryption is the process of converting readable or plain text into a coded or unreadable form, known as ciphertext, using a specific algorithm and key. This ensures that only parties with the correct decryption key can revert the ciphertext back into its original form. In the context of e-business, encryption is crucial for safeguarding sensitive data both during transmission over networks and while stored in databases, effectively reducing the risk of unauthorized access [12].

Among various encryption methods, the Data Encryption Standard (DES) remains a recognized symmetric key algorithm that, despite its age, still offers practical advantages for certain applications [13][14]. DES operates by transforming data into ciphertext using a single shared key for both encryption and decryption. While it may not be suitable for high-security environments requiring advanced cryptographic strength, it remains a viable option for small to medium-sized systems that need a balance between performance and security[15].

This research implements DES encryption in a lightweight, web-based e-business system designed for CV Jasa Karya Rizki. The system is developed to manage customer information and transaction records with security as a built-in feature from the initial design stage. Every piece of sensitive data entered into the system is encrypted before storage, ensuring that the database never holds plain text information. This means that even if the database is compromised, the exposed data would remain unreadable without the correct decryption key.

A distinctive aspect of the system is its real-time decryption feature, which allows authorized users to access original information seamlessly during business operations. When a user with the necessary privileges requests data, the system decrypts it on-the-fly, displays the readable information, and then reverts to storing only the encrypted version in the database. This approach ensures a secure data environment while preserving operational efficiency [16][17]. The ultimate

The IJICS (International Journal of Informatics and Computer Science)
Vol 9 No 2, July 2025, Page 121-127
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

goal of this research is to demonstrate that implementing DES encryption at the point of data entry, combined with secure and efficient decryption for data retrieval, can provide a practical and cost-effective security solution for small business environments. By balancing usability and protection, this system serves as a model for integrating security mechanisms into e-business platforms, ensuring both operational effectiveness and the safeguarding of customer trust in the digital age.

2. RESEARCH METHODOLOGY

2.1 Research Stages

This research was conducted through several stages to ensure a systematic and structured approach in developing and evaluating the e-business system with integrated encryption features. The research began with problem identification, which involved analyzing the needs of CV Jasa Karya Rizki regarding data security in their digital business operations. Following this, a literature review was conducted to gather relevant theories and practices related to information security and cryptographic methods.

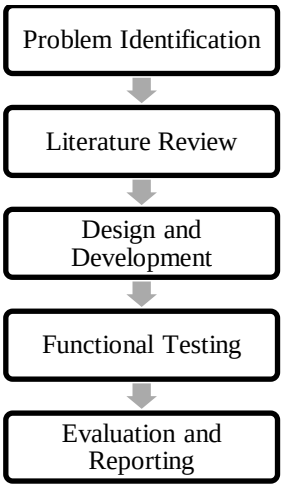


Fig 1. Research Stages

The next stage was the design and development of the web-based e-business application. The system was developed from scratch using PHP for the backend and Bootstrap for the frontend. At this stage, a custom implementation of the DES (Data Encryption Standard) algorithm was integrated to perform encryption and decryption without relying on external libraries. The encryption mechanism was designed to automatically convert input data into ciphertext before saving it into the database. Once the system was developed, functional testing was carried out to ensure that the encryption and decryption processes worked as expected. Data input was tested to verify that encryption occurred before storage, and that decryption could be successfully performed on-the-fly when accessing the data through the user interface. This process also included checking data accuracy and system response during encryption-decryption operations. The final stage of the research involved analyzing the system's performance in handling encrypted data, along with an evaluation of the impact on usability and security. The results were then documented and discussed as part of this paper to highlight the effectiveness of using DES as a data protection mechanism in web-based e-business systems.

2.2 Information System Security

Information system security refers to the practices and technologies used to protect digital data and systems from unauthorized access, use, alteration, or destruction. In the context of web-based applications, especially those involving customer information and transaction records, data security plays a crucial role in ensuring trust and compliance with privacy regulations [18]. Several aspects of information system security must be considered, including confidentiality, integrity, and availability[19]—commonly referred to as the CIA triad. Confidentiality ensures that data is accessible only to authorized users. Integrity refers to the accuracy and completeness of data, while availability ensures that authorized users can access data when needed[20].

Security threats in e-business systems can come from both internal and external sources. Internal threats may include misuse of privileges by employees, while external threats involve hacking, phishing, and unauthorized access attempts. Therefore, implementing technical controls such as encryption, secure authentication, and access control mechanisms is essential to protect critical data within the system. Encryption is one of the most effective techniques for maintaining data confidentiality. It allows sensitive information to be stored in a secure format that cannot be understood without the

The IJICS (International Journal of Informatics and Computer Science)
Vol 9 No 2, July 2025, Page 121-127
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

appropriate decryption key. In information systems, encryption is often used to protect user credentials, transaction records, and personal data stored in databases.

2.3 DES (Data Encryption Standard)

In this study, DES was implemented manually using PHP, without relying on pre-built cryptographic libraries. This approach not only enhances understanding of the internal workings of the algorithm but also allows for full control over the encryption and decryption process. The implementation encrypts customer and transaction data during the input phase and decrypts it temporarily during viewing operations. The choice of DES was based on its simplicity, deterministic behavior, and suitability for small to medium-scale systems. While it may not offer the same level of security as modern algorithms for high-risk applications, it serves effectively in educational systems and controlled environments where system complexity and computational overhead must be minimized. The Data Encryption Standard (DES) is a symmetric block cipher algorithm that encrypts 64-bit blocks of plaintext using a 56-bit key [21]. DES follows the Feistel network structure and performs 16 rounds of encryption, each involving substitution and permutation operations. The algorithm consists of several core stages, as described below:

Initial Permutation (IP)

The plaintext block of 64 bits is subjected to an initial permutation (IP), which rearranges the bits according to a fixed table. This step does not add security but standardizes the input.

$$M \rightarrow IP(M) = L0 \,||\, R0 \quad (1)$$

Key Generation (Key Schedule)

A 56-bit key (excluding 8 parity bits from the original 64-bit input) is used to generate 16 round keys (K1 to K16), each of 48 bits.

$$Ki = PC - 2(LeftShift(Ci - 1) \,||\, LeftShift(Di - 1)) \quad (2)$$

Round Function (f function)

Each of the 16 rounds applies the Feistel function.

$$Li = Ri - 1 \quad (3)$$

$$Ri = Li - 1 \oplus f(Ri - 1, Ki) \quad (4)$$

Final Permutation

After 16 rounds, the final output is the concatenation of R16 and L16 (note the swap). The inverse initial permutation (IP^{-1}) is applied to obtain the ciphertext.

$$Ciphertext = IP^{-1}(R16 \,||\, L16) \quad (5)$$

3. RESULT AND DISCUSSION

3.1 System Design

The system design phase serves as the foundation for the development of the web-based e-business application that incorporates DES encryption to protect customer and transaction data. This phase translates the functional requirements into structured models that guide the development process. Two essential models presented in this section are the Use Case Diagram and the Class Diagram, which illustrate the interaction between users and the system, as well as the internal structure of the system components. These diagrams are used not only to visualize the application's functionality but also to ensure a clear understanding of how data flows through the system, where encryption and decryption processes are applied, and how various components interact with each other.

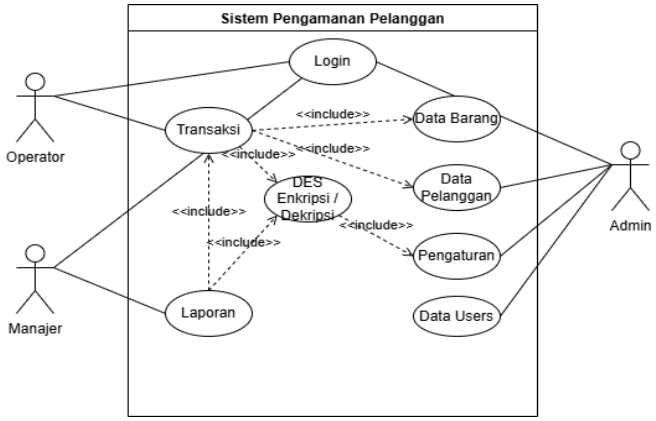


Fig 2. Use Case Diagram

The IJICS (International Journal of Informatics and Computer Science)
Vol 9 No 2, July 2025, Page 121-127
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

The Use Case Diagram illustrates the interactions between users and the functionalities provided by the customer data protection system. The system is accessed by three types of users: Administrator, Operator, and Manager. Each actor is associated with different roles and access permissions based on their responsibilities within the system.

1. Administrator has full access rights to the system. They can manage product data (Data Barang), customer data (Data Pelanggan), user settings (Data Users), and system configurations (Pengaturan). Additionally, the administrator can perform encryption and decryption operations as part of data management processes.
2. Operator interacts with the system primarily for processing Transactions, viewing and inputting Customer Data, and working with the Encryption/Decryption features handled by the integrated DES algorithm. The operator can also access Product Data and view reports as needed.
3. Manager mainly interacts with the Reporting module (Laporan), which aggregates data from transactions and customer records. Although the manager has no direct role in editing data, access to reports may require the system to perform on-the-fly decryption to present readable information.

The encryption and decryption process—represented by the DES Enkripsi/Dekripsi use case—is a core feature and is included in several primary use cases such as transaction processing, customer data handling, and report generation. This ensures that sensitive information is always encrypted before being stored in the system and decrypted only when necessary by authorized users.

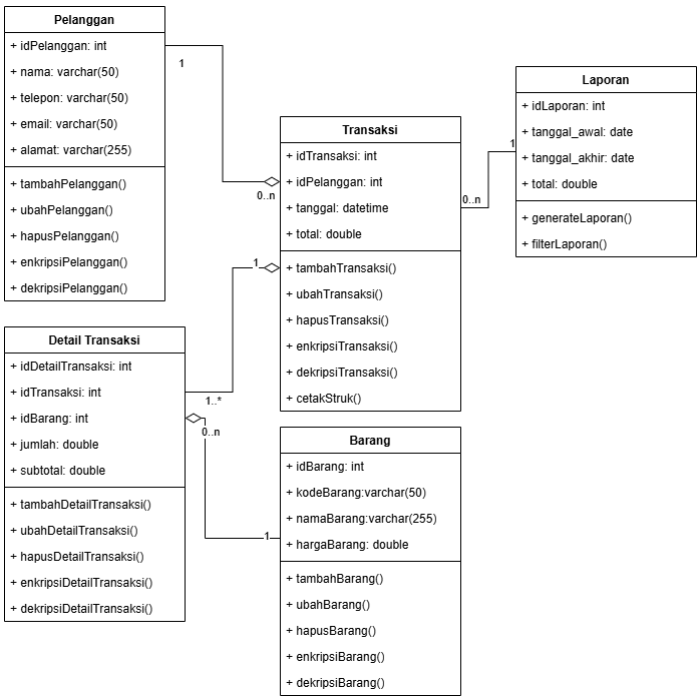


Fig 3. Class Diagram

The Class Diagram provides a structural overview of the system's core components, illustrating how classes are defined and how they interact to manage encrypted customer and transaction data. The system is composed of six primary classes: Pelanggan, Transaksi, DetailTransaksi, Barang, Laporan, and the encryption logic embedded within relevant classes. Each class includes specific attributes and methods tailored to its responsibilities.

1. The Pelanggan (Customer) class holds the personal data of customers, including name, phone number, email, and address. These attributes are subject to encryption during data insertion.

2. The Transaksi (Transaction) class manages customer transactions and is linked with the Pelanggan class through a many-to-one relationship, indicating that each customer can have multiple transactions.

3. The DetailTransaksi (Transaction Detail) class supports the recording of individual transaction items. Each detail entry connects to a transaction and a product, forming a one-to-many relationship with both the Transaksi and Barang classes.

4. The Barang (Product) class stores product-related data, such as product code, name, and price.

The IJICS (International Journal of Informatics and Computer Science)
Vol 9 No 2, July 2025, Page 121-127
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

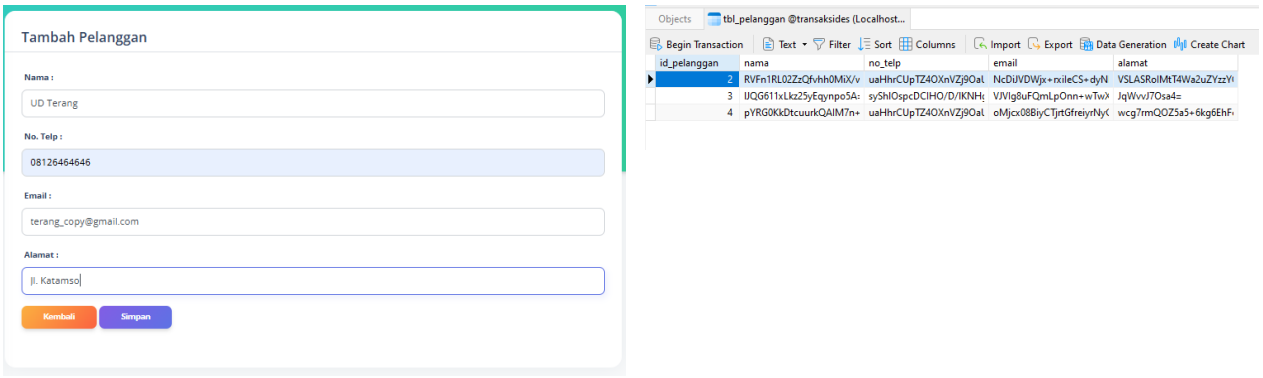
5. The Laporan (Report) class aggregates transaction data for analytical and managerial purposes.

Each of these classes integrates encryption (enkripsi...()) and decryption (dekripsi...()) methods specifically developed using the DES algorithm. The encryption functions are invoked automatically before data is stored in the database, while the decryption functions are triggered on demand when the data needs to be displayed in human-readable form within the user interface.

3.2 System Implementation

The implementation phase focuses on integrating the Data Encryption Standard (DES) algorithm into the core functionality of the e-business system to ensure that customer and transaction data are securely managed. This implementation was developed manually using PHP, without reliance on external cryptographic libraries, providing full control over the encryption and decryption processes.

To demonstrate how data protection is achieved in the system, a simulation of the encryption and decryption process for customer data is presented below. This simulation illustrates how plaintext data entered by users is converted into ciphertext before storage, and how the ciphertext is later decrypted into its original form when needed. During the customer data input phase, the system automatically triggers the DES encryption function upon form submission. The encryption routine is applied to each field deemed sensitive, such as name, phone number, email, and address. The encrypted result is then stored in the database instead of the original input.



(a) (b)

Fig 4. Customer Data Encryption. (a) Input Form, (b) Encrypted Data

In the data listing interface, encrypted data is presented in its ciphertext form by default. This ensures that unauthorized viewers or system users without decryption privileges cannot interpret the stored information. Each row in the table displays the encrypted values of the customer's personal details.

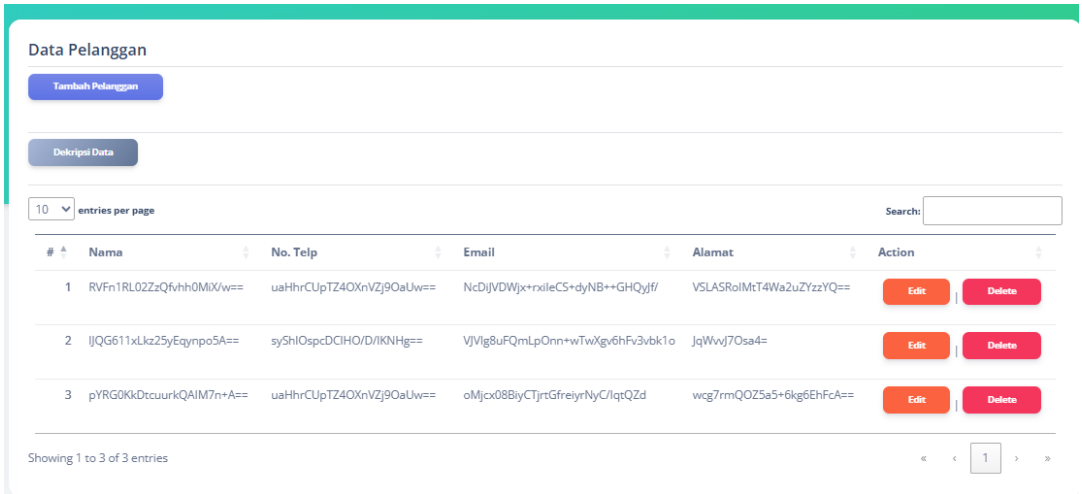


Fig 5. View of Encrypted Customer Data

When an authorized user chooses to view detailed information about a specific customer, the system executes the DES decryption function in real-time. This decrypted data is then rendered on the screen for that session only, without altering the encrypted content stored in the database. This on-the-fly approach ensures both security and convenience.

The IJICS (International Journal of Informatics and Computer Science)
Vol 9 No 2, July 2025, Page 121-127
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

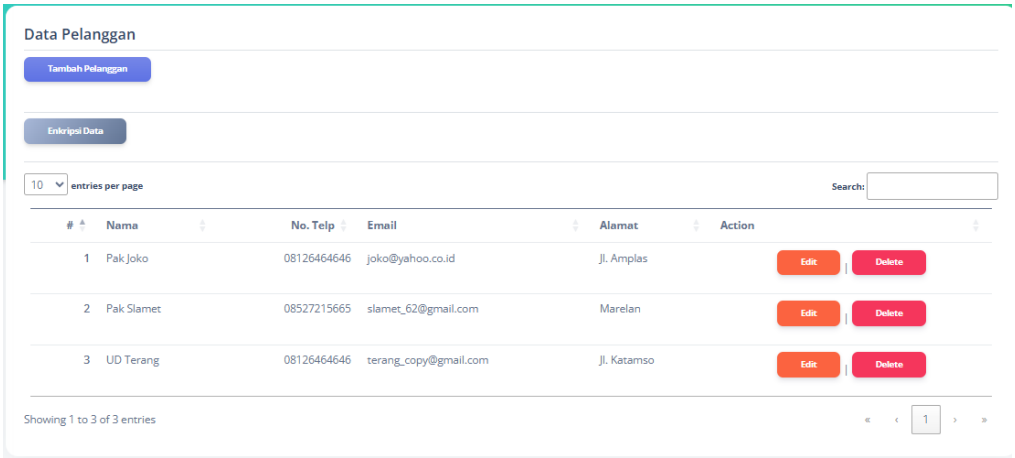


Fig 6. View of Decrypted Customer Data

3.3 Discussion

The implementation of the DES encryption algorithm in this e-business system successfully demonstrates the ability to secure sensitive customer and transaction data during both input and retrieval processes. The system was designed to encrypt data fields such as customer names, addresses, phone numbers, and emails before storing them in the database. The decryption process was executed dynamically, ensuring that plaintext data could be viewed securely without compromising the encrypted records stored in the system.

From the conducted testing and simulations, it was observed that each encryption operation produced consistent and irreversible ciphertext, unless decrypted using the correct key. This confirms the proper functioning of the DES algorithm within the system. Furthermore, the on-the-fly decryption mechanism allowed authorized users to access original data without storing decrypted copies, thereby maintaining the confidentiality and integrity of information.

The encryption process did not introduce significant delays or degrade system performance. This is due to the lightweight design of the DES algorithm, which is well-suited for small to medium-sized web applications like the one developed in this study. The use of custom PHP-based DES logic also ensured seamless integration with the system's existing modules, without dependency on external libraries or frameworks.

In addition to the technical success, the integration of encryption as part of the data workflow promotes good security practices. By encrypting data at the point of input, the system ensures that even if unauthorized access to the database occurs, the exposed data remains unreadable. This approach aligns with best practices in information security and prepares the system for compliance with emerging data protection regulations.

One of the strengths of the implemented system is its modular design. Encryption and decryption functions were encapsulated within each relevant class, such as Pelanggan, Transaksi, and Barang. This makes the system highly maintainable and allows future developers to extend encryption logic to additional modules or adopt alternative algorithms like AES or RSA if needed.

However, while DES served its purpose effectively in this project, it is important to note that DES is no longer considered secure for large-scale or high-risk applications due to its short key length. In a production environment handling sensitive data on a national or global scale, stronger algorithms with longer key lengths and resistance to brute-force attacks should be considered.

4. CONCLUSION

This study has successfully developed a web-based e-business application with an integrated customer data encryption feature using the Data Encryption Standard (DES) algorithm. The system was designed to securely manage customer and transaction information by encrypting sensitive data before it is stored in the database and decrypting it on demand during authorized access. The encryption and decryption processes were implemented manually using PHP, allowing for a deeper

ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v9i2.8999

understanding of DES logic and providing full control over its application. Simulation and system testing confirmed that data encryption was applied correctly during the input phase and decryption was performed accurately during the data viewing phase. As a result, the confidentiality and privacy of customer data were preserved without affecting system performance or usability. This approach proved effective in demonstrating how classic cryptographic techniques like DES can be integrated into a modern web application to enhance data protection, especially in small business environments where lightweight solutions are preferred. The modular architecture of the system ensures maintainability and allows for future upgrades, including the potential adoption of more secure encryption standards. Overall, the system fulfills its main objective of providing a secure digital environment for CV Jasa Karya Rizki, minimizing the risks of data breaches and unauthorized access while ensuring that business operations remain efficient and user-friendly.

REFERENCES

[1] E. Lulaj, "a Sustainable Business Profit Through Customers and Its Impacts on Three Key Business Domains: Technology, Innovation, and Service (Tis)," *Business, Manag. Econ. Eng.*, vol. 21, no. 1, pp. 19–47, 2023.
[2] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of E-Business Information System in Indonesia : Prospects and Challenges," *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 2, pp. 180–188, 2021.
[3] S. K. Krishnakumar, R. Kishore, and N. C. Suresh, "Expansive or focused attention? An exploration–exploitation perspective on e-Business systems and firm performance," *Prod. Oper. Manag.*, vol. 31, no. 5, pp. 2038–2066, 2022.
[4] M. Krasnyuk, Y. Kulynych, V. Tuhaienko, and S. Krasniuk, "E-Business and E-Commerce Technologies As an Important Factor for Economic Efficiency and Stability in the Modern Conditions of the Digital Economy (on the Example of Oil and Gas Company)," in *Grail of Science*, 2022, no. 17, pp. 69–81.
[5] C. Liao, "Do E-Business Services Enhance Bank Efficiency in Taiwan?," *Int. J. Inf. Syst. Serv. Sect.*, vol. 14, no. 1, pp. 1–17, 2022.
[6] M. R. S. Mohan Reddy Sareddy, "Cloud-Based Customer Relationship Management: Driving Business Success in the E-Business Environment," *Int. J. HRM Organ. Behav.*, vol. 15, no. 2, pp. 1–16, 2023.
[7] Nduji Romanus, Marcus Garvey Orji, Oyenuga Michael Oyedele, and Oriaku Chris, "Assessing E-business and Organizational Performance in Nigeria Today: Evidence from Jumia Ltd, Lagos," *Britain Int. Humanit. Soc. Sci. J.*, vol. 5, no. 2, pp. 81–92, 2023.
[8] A. S. Edu, D. Agozie, and M. Agoyi, "Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis," *PeerJ Comput. Sci.*, vol. 7, pp. 1–26, 2021.
[9] P. Sharma and H. Gupta, "Emerging Cyber Security Threats and Security Applications in Digital Era," in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2024*, 2024, pp. 1–6.
[10] C. Asbaş and Ş. Tuzlukaya, "Cyberattack and cyberwarfare strategies for businesses," in *Conflict Management in Digital Business: New Strategy and Approach*, Emerald Publishing Limited, 2022, pp. 303–328.
[11] K. Bhakhri, M. Sethi, I. Sharma, and K. Kaushik, "Examining the Consequences of Cyberattacks on Businesses and Organizations," in *Lecture Notes in Networks and Systems*, 2024, vol. 972, pp. 227–239.
[12] H. Taherdoost, "E-Business Security and Control," in *EAI/Springer Innovations in Communication and Computing*, vol. Part F1354, Springer, 2023, pp. 105–135.
[13] P. Matta, M. Arora, and D. Sharma, "A comparative survey on data encryption Techniques: Big data perspective," *Mater. Today Proc.*, vol. 46, pp. 11035–11039, 2021.
[14] Omolara Patricia Olaiya, Temitayo Oluwadamilola Adesoga, Azeez Adekunle Adebayo, Fehintola Moyosore Sotomi, Oluwaseun Aaron Adigun, and Paschal M Ezeliora, "Encryption techniques for financial data security in fintech applications," *Int. J. Sci. Res. Arch.*, vol. 12, no. 1, pp. 2942–2949, 2024.
[15] T. S. Alasi and M. Halim, "Pengujian Algoritma Kriptografi Rijndael Untuk Keamanan Audio Menggunakan Visual Basic .Net," *J. Informatics Log.*, vol. 1, no. 1, pp. 8–17, 2024.
[16] N. P. Hemanth Kumar and S. Prabhudeva, "Layers Based Optimal Privacy Preservation of the On-premise Data Supported by the Dual Authentication and Lightweight on Fly Encryption in Cloud Ecosystem," *Wirel. Pers. Commun.*, vol. 121, no. 3, pp. 1489–1508, 2021.
[17] H. Dubey, S. Kumar, and A. Chhabra, "Cyber security model to secure data transmission using cloud cryptography," *Cyber Secur. Insights Mag.*, vol. 2, pp. 9–12, 2022.
[18] A. Georgiadou, S. Mouzakitis, K. Bounas, and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," *J. Comput. Inf. Syst.*, vol. 62, no. 3, pp. 452–462, 2022.
[19] T. S. Alasi, "Algoritma Hill Cipher Untuk Kebenaran Informasi pada Gambar dalam Media Sosial," *J. Inf. Komput. Log.*, vol. 2, no. 2, 2021.
[20] T. S. Alasi, *Ilmu Komputer*, 1st ed. Deli Serdang, 2024.
[21] Z. Yuan and C. Lin, "Research on Strong Constraint Self-training Algorithm and Applied to Remote Sensing Image Classification," in *Proceedings of 2021 IEEE International Conference on Power Electronics, Computer Applications, ICPECA 2021*, 2021, pp. 981–985.