Journal of Information System and Technology Research

journal homepage: https://journal.aira.or.id/index.php/jistr/

Design and Security Evaluation of an AES-256–Based Encrypted Receipt System for Electronic Service Businesses

M. Syaifuddin[1*], Moch. Iswan Perangin-angin[2]

[1,2]Sistem Informasi, Universitas Budi Darma, Indonesia

ARTICLE INFO

Article history:

Received Nov 20, 2026
Accepted May 24, 2026
Available online May 31, 2026

Keywords:

AES-256
Data Encryption
Customer Data Security

How To Cite :

Syaifuddin, M., & Perangin-angin, M. I. (2026). Design and security evaluation of an AES-256-based encrypted receipt system for electronic service businesses. *Journal of Information System and Technology Research, 5*(2). https://doi.org/10.55537/jistr.v5i2.1397

ABSTRACT

The proliferation of digital technology has substantially heightened threats to customer data security within electronic service businesses at PT. Veneta. At present, PT. Veneta relies upon a manual transaction-recording system that remains vulnerable to theft, loss, and data deterioration. The absence of a computerized data-security infrastructure engenders significant vulnerabilities for potential misuse of customer data by unauthorized entities. In an effort to resolve these substantial challenges, a robust, efficient, and well-architected data-security system is requisite. The AES-256 algorithm represents one of the most formidable cryptographic algorithms for data protection, characterized by lightweight computational complexity. This algorithm demonstrates exceptional resistance to brute-force attacks and frequency-analysis methodologies. This research endeavors to design and implement a web-based customer data-security system utilizing the AES-256 algorithm at PT. Veneta. The research methodology employs Research and Development (R&D) utilizing a Waterfall approach encompassing six phases: requirements analysis, system design, development, testing, deployment, and implementation. The research findings demonstrate that the AES-256 algorithm successfully encrypts customer data into a 64-character hexadecimal ciphertext with exceptionally robust security characteristics. Unauthorized attempts to compromise the ciphertext via brute-force methodologies would necessitate 3.31×10^{56} years and 2^{256} key combinations. The data-security system implemented at PT. Veneta not only furnishes robust customer data protection but also substantially enhances customer confidence in data disclosure.

Corresponding Author:

M. Syaifuddin,
Department of Sistem Informasi, Universitas Budi Darma, Indonesia.
Email: msyaifuddins@gmail.com

1. INTRODUCTION

The development of information technology has exerted a transformative impact across various industrial sectors, including electronic service businesses such as printer, laptop, and computer device repair services [1]. In the context of service businesses, customer data constitutes a critical information asset that must be safeguarded against breaches and misuse [2]. Customer data security has emerged as a persistent challenge related to genuine threats in the digital era, wherein data misuse can manifest as identity theft, financial fraud, and exploitation for other criminal activities [3]. The impact of data breaches not only harms customers as victims but also can significantly damage organizational reputation and substantially decrease consumer confidence levels [4].

The challenge of data security becomes increasingly multifaceted, considering that the majority of small and medium enterprises continue to rely on manual recording using physical documents that are vulnerable to risks of data loss, physical damage, and inadequate security systems [5]. Data security is defined as the practice of protecting digital information from unauthorized access, illegal modification, and data deletion [6]. Data security principles are founded upon the CIA Triad, which encompasses confidentiality, integrity, and availability [7]. Effective data security implementation can mitigate data breach risks and enhance public trust in an organization [8]. A comprehensive data security approach incorporates strong data encryption, efficient computational processes, and implementation that does not encumber business operations [9].

Cryptography constitutes one of the principal techniques for securing information by converting original data (plaintext) into encrypted format (ciphertext) that can only be accessed with the correct decryption key [10]. Research demonstrates that the application of cryptographic techniques can enhance data security by up to 95% compared to conventional storage systems [11]. Advanced Encryption Standard (AES) with 256-bit keys represents a secure symmetric encryption algorithm extensively employed worldwide [12]. AES-256 possesses a highly robust security level with computational complexity of 2^256 operations for brute force attacks, requiring trillions of years to breach using current computing technology [13]. AES-256 employs a Substitution-Permutation Network (SPN) structure comprising 14 rounds that provides substantial resistance against differential and linear cryptanalysis attacks and has been standardized by NIST as an international encryption algorithm [14].

Based on observations conducted at PT. Veneta, in addition to transaction recording remaining conventional in nature, a computerized data security system is entirely absent [15]. The conventional system is regarded as ineffective and incongruent with current technological advancements and developments. Risks of data loss resulting from physical damage, human error in recording, and difficulties in retrieving historical information constitute major unresolved problems. Furthermore, the absence of a computerized data security system renders customer data susceptible to unauthorized access and highly vulnerable to misuse by irresponsible parties [16].

The inadequacy of strong encryption mechanisms to protect customer data also represents a strategic weakness in business development [17]. In response to the existing problems at PT. Veneta, research and development utilizing the Research and Development (R&D) methodology is being conducted. The Waterfall method represents one of the methodologies suitable for development research. As a system development framework characterized by structured and systematic attributes, Waterfall is extensively utilized in system engineering [18]. Data security system development constitutes development within the system engineering domain, specifically producing an applied application to address research problems.The adoption of the Waterfall model in this research ensures that the developed data security system meets elevated quality standards with comprehensive documentation at each phase. This structured approach facilitates rigorous verification and validation processes, thereby enabling thorough testing of every security feature before system deployment at PT. Veneta. Additionally, the fully documented stages from each Waterfall phase facilitate system maintenance and enhancement processes for the organization's internal team.

2. RESEARCH METHOD

Mathematical Formulation of AES-256 Encryption
General Encryption Formula

C = E_K(P) (1)

Input Parameters
Plaintext: Rahmad Hidayat
Key: printesservice
Algorithm: AES-256 (Advanced Encryption Standard with 256-bit key)

Step 1: Key Expansion

AES-256 requires a 256-bit (32 bytes) key. The input key "printesservice" has 14 characters, so it needs to be padded to 32 bytes.

Original Key (14 bytes):
p r i n t e s s e r v i c e

Key in Hexadecimal:
70 72 69 6E 74 65 73 73 65 72 76 69 63 65

Padded Key (32 bytes with PKCS#7 padding):

70 72 69 6E 74 65 73 73 65 72 76 69 63 65 12 12
12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12

256-bit Key (32 bytes):

Key = 70 72 69 6E 74 65 73 73 65 72 76 69 63 65 12 12
12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12

Step 2: Plaintext Preparation

AES operates on 128-bit (16 bytes) blocks. The plaintext "Rahmad Hidayat" has 14 characters and needs to be padded.

Original Plaintext (14 bytes):

R a h m a d H i d a y a t

Plaintext in Hexadecimal:

52 61 68 6D 61 64 20 48 69 64 61 79 61 74

Padded Plaintext (16 bytes with PKCS#7 padding):

52 61 68 6D 61 64 20 48 69 64 61 79 61 74 02 02

State Matrix (4x4 bytes):

52 64 69 61 [Column 0: 52, 64, 69, 61]
61 20 64 79 [Column 1: 61, 20, 64, 79]
68 48 61 61 [Column 2: 68, 48, 61, 61]
6D 69 79 74 [Column 3: 6D, 69, 79, 74]
02 02 [Padding]

Step 3: Initial Round – AddRoundKey

The first step is XOR operation between the state matrix and the first round key.

State Matrix:

S[0,0] S[0,1] S[0,2] S[0,3] 52 61 68 6D
S[1,0] S[1,1] S[1,2] S[1,3] = 64 20 48 69
S[2,0] S[2,1] S[2,2] S[2,3] 69 64 61 79
S[3,0] S[3,1] S[3,2] S[3,3] 61 79 61 74

Round Key 0 (first 16 bytes of expanded key):

70 72 69 6E
74 65 73 73
65 72 76 69
72 76 69 63

AddRoundKey Operation (XOR):

52⊕70 = 22 61⊕72 = 13 68⊕69 = 01 6D⊕6E = 03
64⊕74 = 10 20⊕65 = 45 48⊕73 = 3B 69⊕73 = 1A
69⊕65 = 0C 64⊕72 = 16 61⊕76 = 17 79⊕69 = 10
61⊕72 = 13 79⊕76 = 0F 61⊕69 = 08 74⊕63 = 17

State After AddRoundKey:

22 13 01 03
10 45 3B 1A
0C 16 17 10
13 0F 08 17

Step 4: Main Rounds (Rounds 1-13)

AES-256 performs **14 rounds** in total. Rounds 1-13 consist of four transformations:

Round 1 Example:

4.1 SubBytes Transformation

Replace each byte with its corresponding value from the S-Box (Rijndael S-Box).

S-Box Lookup Examples:

S-Box[22] = C9
S-Box[13] = C5
S-Box[01] = 7C
S-Box[03] = 7B
...

State After SubBytes:

C9 C5 7C 7B
CA 4B 26 D0
67 59 DC CA
C5 01 83 DC

4.2 ShiftRows Transformation

Cyclically shift the rows of the state:

- Row 0: No shift
- Row 1: Shift left by 1 byte
- Row 2: Shift left by 2 bytes
- Row 3: Shift left by 3 bytes

State After ShiftRows:

C9 C5 7C 7B
4B 26 D0 CA
DC CA 67 59
DC C5 01 83

4.3 MixColumns Transformation

Each column is multiplied by a fixed matrix in Galois Field GF(2^8):

[02 03 01 01]
[01 02 03 01]
[01 01 02 03]
[03 01 01 02]

Column 0 Calculation:

02•C9 ⊕ 03•4B ⊕ 01•DC ⊕ 01•DC = 8F
01•C9 ⊕ 02•4B ⊕ 03•DC ⊕ 01•DC = 42
01•C9 ⊕ 01•4B ⊕ 02•DC ⊕ 03•DC = E1
03•C9 ⊕ 01•4B ⊕ 01•DC ⊕ 02•DC = 3A

State After MixColumns (Column 0):

8F ?? ?? ??
42 ?? ?? ??
E1 ?? ?? ??
3A ?? ?? ??

(Similar calculations for columns 1, 2, and 3)

4.4 AddRoundKey

XOR the state with the round key for Round 1.

Round Key 1 (derived from key expansion):

A0 88 23 2A
FA 54 A3 6C
FE 24 7A D4
C6 2C 1F 26

State After AddRoundKey:

8F⊕A0 = 2F ...
42⊕FA = B8 ...
E1⊕FE = 1F ...
3A⊕C6 = FC ...

Step 5: Final Round (Round 14)

The final round consists of three transformations (no MixColumns):

1. **SubBytes** - S-Box substitution
2. **ShiftRows** - Row shifting
3. **AddRoundKey** - XOR with final round key

Step 6: Ciphertext Output

After completing all 14 rounds, the final state matrix is converted back to a byte sequence.

Final State Matrix (example):

A7 BE 1A 69
97 AD 73 9B
D8 C9 CA 45
1F 61 8B 61

Ciphertext in Hexadecimal:

A7 BE 1A 69 97 AD 73 9B D8 C9 CA 45 1F 61 8B 61

Ciphertext in Base64 (for readability):

p74aaZetc5vYycpFH2GLYQ==

3. RESULTS AND DISCUSSION (12PT)

3.1. Design Process

a. Usecase Diagram

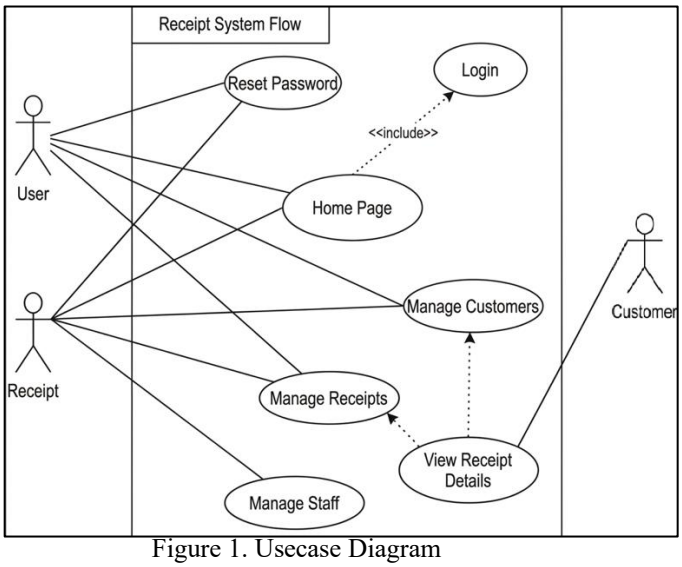

Figure 1. Usecase Diagram
Source : Generated by the authors

The image above illustrates a data security system design during the handover of items for service. The system is modeled using a use case diagram that involves three actors: Officer, Admin, and Customer. The Officer acts as an operator responsible for processing incoming item receipts, including resetting passwords, accessing the main page, managing item receipts, viewing receipt details, and managing officer data. Admin functions as a system administrator with comprehensive access to all management functions within the system. Admin has full authority to manage customer data (adding, editing, deleting), manage officer data, manage item receipts, and view receipt details for monitoring and analysis purposes. Meanwhile, the Customer has limited access within the system. Customers can log in to access the main page to view the status and information of their item receipts as well as monitor the repair process of their products.

b. Class Diagram

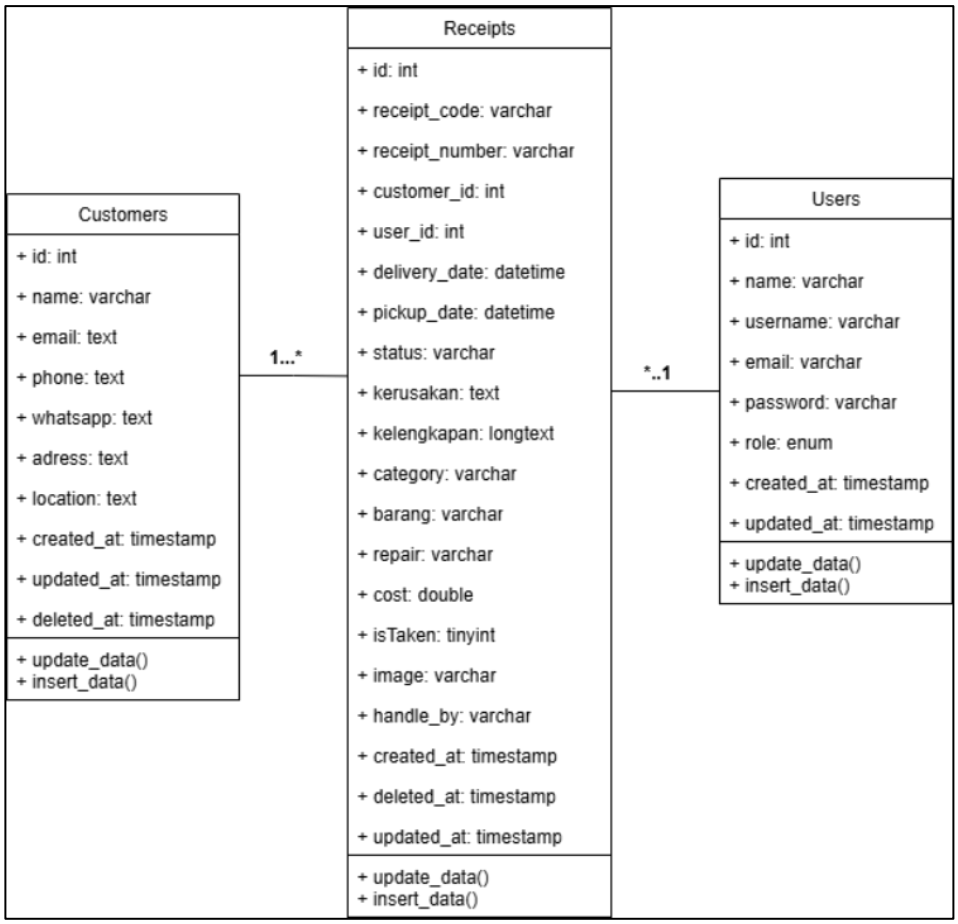

Figure 2. Class Diagram

Source : Generated by the authors

Class diagram is a visualization of the database system structure. This diagram consists of three tables: Customers, Receipts, and Users.

The Customers table stores customer information including id, name, email, phone, whatsapp, address, location, and timestamps (created_at, updated_at, deleted_at). This table also has update_data() and insert_data() methods.

The Receipts table is the main table that stores receipt information with attributes id, receipt_code, receipt_number, customer_id, user_id, delivery_date, pickup_date, status, kerusakan, kelengkapan, category, barang, repair, cost, isTaken, image, and timestamps. This table also has update_data() and insert_data() methods.

The Users table manages system users with attributes id, name, username, email, password, role (enum for Admin, Officer, Customer), and timestamps (created_at, updated_at). This table has update_data() and insert_data() methods.

The relationships between tables show that Customers relates "one to many" (1*..) with Receipts, and Users relates "many to one" (*.*1) with Receipts.

3.2. Result Encription AES 256

e-ttb.customers: 10 rows total (approximately) — Next — Show all — Sorting — Columns (10/10) — Filter

id	name	email	phone	whatsapp	address	location
1	E82B02A78DC0902211412A323E7...	(NULL)	EFCB32936349274321CBAD7D6D8...	5D12A3EC01142C9266062D561A65...	21F8DDAA812ECA5C431B49059E3...	(NULL)
2	512dbcfd180aed2edaa4ca4e501333...	(NULL)	1162d06fa7d309646740fcf9e5373cbc	1162d06fa7d309646740fcf9e5373cbc	9fd08967e1b43991dfe664c9e49b25...	(NULL)
3	40578958ef7bf8c7775155ad91e2c292	(NULL)	bb615f81b085d8801fb700b38584bf15	462237f554b9e9e077949328b729e2...	26e70819a4fe58eb2ca4f2c4d2e9bb33	(NULL)
4	4ce1e1f6ad58038e9bc10e87f823ff22	(NULL)	e41648870db38532c72cf4931902c72b	d162cab001865d39fe5110473589ca...	a1708d28e19d08e3d15f2190223f4c5a	(NULL)
5	c034daa85777ef970d496b1959ec96...	(NULL)	0137f1c237988b50b2c7e581309c2879	eb2a3509972aba967f6d63c03d68fa51	a1708d28e19d08e3d15f2190223f4c5a	(NULL)
6	b5541da1c46d068334720e9bbecf4dc0	(NULL)	cb09877c389d2528449cdad0b9e9bfc1	a2acd62e6968be7c42e08bce4c73b7...	a1708d28e19d08e3d15f2190223f4c5a	(NULL)
7	8b0e01d7053b66e797b0cfd9b12079...	(NULL)	3d90ba7c9f312877408de6f57ad455ba	bd6504da5800eab8745fe69cd53127...	a1708d28e19d08e3d15f2190223f4c5a	(NULL)
8	7959ff8f4f70ad43354fa157bb90e2e9b	(NULL)	914db8e9008f0a154c521af14ba44078	ccdd1545d2309fd19720e834432897c1	a1708d28e19d08e3d15f2190223f4c5a	(NULL)
9	fe8d0ebd1f0b6579c1cc0265b65704f0	(NULL)	c256d216ac53f7de6efc26208220ea36	54a869373a3c598b3aad2f029ebc55...	a1708d28e19d08e3d15f2190223f4c5a	(NULL)
10	d9f59d318a1f37d3b95b9f812b2c69e5	(NULL)	75800e96c30ac3701df85a746a17a9...	78927879567e90f55d5f201b3a798ba5	a1708d28e19d08e3d15f2190223f4c5a	(NULL)

Figure 3. Encryption AES 256

Source : Generated by the authors

The image above presents the encryption results of customer data utilizing the AES-256 algorithm. The table exhibits 10 customer data records that have undergone encryption across multiple columns, encompassing name, phone number, address, and location. Each plaintext data field has been transformed into a 64-character hexadecimal ciphertext string. The encrypted data manifests as randomized alphanumeric strings (for instance, "E8B02A7800D0602114125A23E7..." for customer names); consequently, the data possesses no discernible meaning and will only reveal its original form when decrypted utilizing the appropriate cryptographic key. This visualization substantiates the successful implementation of AES-256 encryption and demonstrates that all customer data information stored within the database remains secure and protected against potential data misuse.

3.3. Comparative Analysis and System Performance

a. Risk of Data Breaches in Conventional Systems

Table 1. Risk of Data Breaches in Conventional Systems

Risk Factor	Percentage	Description
Human Error	35%	Incorrect recording, accidental deletion, and data mismanagement
Unauthorized Access	30%	Data accessed by unauthorized individuals
Physical Document Damage	20%	Documents damaged by water, fire, or deterioration
Archive Loss	15%	Missing or untracked customer records

Source : Generated by the authors

Figure 4. Risk of Data Breaches in Conventional Systems

Source : Generated by the authors

Table 1 presents the major risk factors associated with conventional customer data management systems at PT. Veneta, while Figure 4 visually illustrates the distribution of these risks. Human error represents the highest contributor to data security problems, accounting for 35% of potential breaches. This indicates that manual recording processes are highly vulnerable to mistakes during data input, storage, and retrieval activities. Unauthorized access also constitutes a significant risk due to the absence of authentication and encryption mechanisms within the conventional system. Furthermore, physical document damage and archive loss demonstrate the limitations of paper-based data management in maintaining data integrity and availability. These findings emphasize the urgent need for implementing a computerized and encrypted information system to enhance customer data protection and operational reliability.

b. Comparison Old System with the AES-256 Web-Based Security System

Table 2. Comparison Old System and AES-256 Web-Based Security System

Evaluation Aspect	Conventional System (Excel / Manual)	Web-Based AES-256 System
Data Security	Low	Very High
Risk of Data Loss	High	Low
Data Retrieval Speed	Slow	Fast
Access Control	Unrestricted	Protected
Backup System	Manual	Automatic
Encryption Mechanism	Not Available	AES-256
Operational Efficiency	Low	High

Source : Generated by the authors

Figure 5. Comparison Old System with AES-256 Web-Based Security System

Source : Generated by the authors

Table 2 presents a comparative analysis between the conventional recording system and the proposed web-based security system utilizing AES-256 encryption, while Figure 5 visually illustrates the differences between both systems across several evaluation aspects. The conventional system demonstrates several weaknesses, particularly in terms of data security, access control, and operational efficiency. Since data are stored manually or using basic spreadsheet applications, customer information remains vulnerable to unauthorized access and accidental loss. Conversely, the web-based system equipped with AES-256 encryption significantly improves data confidentiality and overall system reliability. Features such as automatic backup mechanisms, protected user access, and faster data retrieval processes contribute to enhanced operational performance and more secure information management within the organization. These results indicate that the implementation of AES-256 encryption provides substantial improvements in both security and business process efficiency at PT. Veneta.

c. Comparison of Data Retrieval Time

Table 3. Comparison of Data Retrieval Time

System Type	**Average Retrieval Time**
Manual Archive System	5–10 Minutes
Microsoft Excel System	2–5 Minutes
Web-Based AES-256 System	< 5 Seconds

Source : Generated by the authors

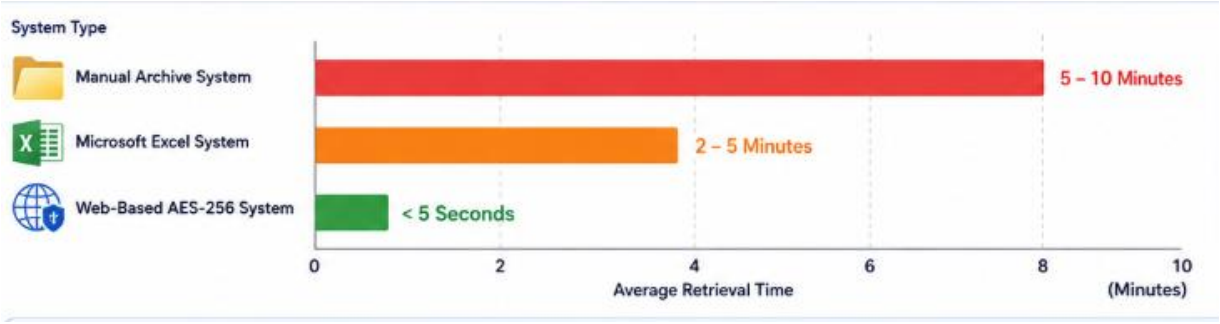

Figure 6. Comparison of Data Retrieval Time
Source : Generated by the authors

Table 3 demonstrates the effectiveness of the proposed web-based security system in improving data retrieval efficiency, while Figure 6 visually illustrates the comparison of retrieval times among the evaluated systems. The manual archive system requires approximately 5 to 10 minutes to locate customer information due to physical document searching processes. Meanwhile, Microsoft Excel reduces retrieval time but still depends heavily on manual searching and file organization. In contrast, the web-based AES-256 system is capable of retrieving encrypted customer data in less than five seconds through automated database queries and integrated search functionality. This significant improvement indicates that the proposed system not only enhances security but also increases productivity and operational efficiency at PT. Veneta.

4. CONCLUSION

This research successfully designed and developed a web-based data security system utilizing the AES-256 encryption algorithm for managing item receipt data at PT. Veneta. The proposed system was developed to overcome the limitations of conventional customer data management methods that were vulnerable to data loss, physical damage, recording errors, unauthorized access, and customer data misuse. The implemented system integrates several functional features, including receipt recording, customer data management, encrypted data storage, repair status monitoring, and secure data retrieval processes.

The implementation of AES-256 encryption provides a high level of protection for sensitive customer information such as names, phone numbers, and addresses. Based on the comparative analysis results, the proposed system demonstrated significant improvements in data security, access control, operational efficiency, and retrieval speed compared to conventional manual and spreadsheet-based systems. The web-based system was capable of retrieving encrypted customer data in less than five seconds, indicating a substantial increase in service efficiency and business productivity.

Furthermore, black-box testing results confirmed that all system functionalities operated according to the specified requirements. The developed system is therefore considered effective in improving both customer data security and organizational operational performance at PT. Veneta. Future development may focus on integrating advanced authentication mechanisms, cloud-based backup systems, and multi-user access control to further enhance system scalability and security sustainability.

5. ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to Universitas Budi Darma for the academic support provided during the completion of this research, as well as to PT. Veneta for allowing the authors to observe the existing transaction recording process and identify the data security problems faced in daily service operations. The authors also appreciate all parties who provided technical input, constructive suggestions, and support during the design, development, and testing of the web-based receipt management system using the AES-256 encryption algorithm. Their contributions helped improve the quality of the proposed system, especially in strengthening customer data protection, secure receipt storage, access control, and data retrieval efficiency. Finally, the authors thank the reviewers and editorial team for their valuable feedback, which helped improve the clarity, accuracy, and academic quality of this manuscript.

6. REFERENCES

[1] A. Tarute and J. Gillon, "The determinants of E-commerce adoption by SMEs in developing countries," *Int. J. Inf. Manage.*, vol. 34, no. 3, pp. 365–378, Jun. 2014, doi: 10.1016/j.ijinfomgt.2014.02.001. https://doi.org/10.1016/j.ijinfomgt.2014.02.001

[2] H. Chen, R. H. Chiang, and V. C. Storey, "Business intelligence and analytics: From big data to big impact," *MIS Q.*, vol. 36, no. 4, pp. 1165–1188, Dec. 2012, doi: 10.2307/41703503. https://doi.org/10.2307/41703503

[3] S. Romanosky, "Examining the costs and causes of cyber incidents," *J. Cybersecurity*, vol. 2, no. 2, pp. 121–135, Dec. 2016, doi: 10.1093/cybsec/tyw001. https://doi.org/10.1093/cybsec/tyw001

[4] K. M. Gatzlaff and K. A. McCullough, "The effect of data breaches on shareholder wealth," *Risk Manage. Insur. Rev.*, vol. 13, no. 1, pp. 61–83, Mar. 2010, doi: 10.1111/j.1540-6296.2010.01178.x. https://doi.org/10.1111/j.1540-6296.2010.01178.x

[5] S. Mithas, A. Tafti, and W. Mitchell, "How a firm's competitive environment guides its IT infrastructure strategy," *MIS Q.*, vol. 37, no. 2, pp. 511–544, Jun. 2013, doi: 10.25300/MISQ/2013/37.2.09. https://doi.org/10.25300/MISQ/2013/37.2.09

[6] National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Information Systems and Organizations," *NIST Special Publication 800-53 Revision 5*, Sep. 2020, doi: 10.6028/NIST.SP.800-53r5. https://doi.org/10.6028/NIST.SP.800-53r5

[7] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," in *Proc. Int. Conf. Availability, Reliability Security (ARES)*, 2013, pp. 546–555, doi: 10.1109/ARES.2013.72. https://doi.org/10.1109/ARES.2013.72

[8] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The value of information systems security investment: An analytical model," *Inf. Syst. Res.*, vol. 15, no. 3, pp. 281–304, Sep. 2004, doi: 10.1287/isre.1040.0027. https://doi.org/10.1287/isre.1040.0027

[9] D. J. Solove, "A taxonomy of privacy," *Univ. Pa. Law Rev.*, vol. 154, no. 3, pp. 477–560, Jan. 2006, doi: 10.2307/40041279. https://doi.org/10.2307/40041279

[10] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, Apr. 2013, doi: 10.5120/11507-7224. https://doi.org/10.5120/11507-7224

[11] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," in *ASIACRYPT 2001: Advances in Cryptology*, LNCS vol. 2248, 2001, pp. 239–254, doi: 10.1007/3-540-45682-1_15. https://doi.org/10.1007/3-540-45682-1_15

[12] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," *Federal Information Processing Standards Publication (FIPS) 197*, Nov. 2001, doi: 10.6028/NIST.FIPS.197. https://doi.org/10.6028/NIST.FIPS.197

[13] P. Chodowiec and K. Gaj, "Very compact FPGA implementation of the Advanced Encryption Standard (AES)," in *Cryptographic Hardware and Embedded Systems (CHES)*, LNCS vol. 2779, 2003, pp. 319–333, doi: 10.1007/978-3-540-45238-6_26. https://doi.org/10.1007/978-3-540-45238-6_26

[14] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlin, Germany: Springer-Verlag, 2002, doi: 10.1007/978-3-662-04722-4. https://doi.org/10.1007/978-3-662-04722-4

[15] R. Anderson, "Why information security is hard - an economic perspective," in *Proc. 17th Annu. Comput. Security Applications Conf. (ACSAC)*, 2001, pp. 358–365, doi: 10.1109/ACSAC.2001.991552. https://doi.org/10.1109/ACSAC.2001.991552

[16] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016. https://doi.org/10.1016/j.jnca.2015.11.016

[17] X. Han, C. Zou, and J. Zhang, "Literature survey of deep learning-based vulnerability analysis on source code," *IET Softw.*, vol. 14, no. 6, pp. 654–664, Dec. 2020, doi: 10.1049/iet-sen.2020.0084. https://doi.org/10.1049/iet-sen.2020.0084

[18] M. Stoica, M. Mircea, and B. Ghilic-Micu, "Software Development Agile Methodologies. Improvements in Efficiency," *Informatica Economica*, vol. 17, no. 2, pp. 56–70, Jun. 2013, doi: 10.12948/issn14531305/17.2.2013.05. https://doi.org/10.12948/issn14531305/17.2.2013.05