Journal of Technology and Informatics (JoTI)
Vol. 7, No. 1, Bulan April Tahun 2025
P-ISSN 2721-4842
E-ISSN 2686-6102

Strengthening Web-Based Login Security Using Vigenère Cipher and AES ENCRYPT() Method in MySQL

Rhendy Diki Nugraha[1*], Muhamad David Ali[2], Nadya Khairunissa[3], Danang Nurcahyo[4], Ahmad Turmudi Zy[5]

[1,2,3,4,5]Informatics Engineering, Pelita Bangsa University, Bekasi, Indonesia
e-mail: rendydikinugraha@gmail.com[1], kingawpbekasi@gmail.com[2], nadyakhorun13@gmail.com[3], danangpaten1@gmail.com[4], turmudi@pelitabangsa.ac.id[5]

Article Information

Article History:

Received	: January 7th, 2025
Revised	: Maret 20th, 2025
Accepted	: April 29th, 2025
Published	: April 30th, 2025

***Correspondence:**
rendydikinugraha@gmail.com

Keywords:
AES_ENCRYPT(), Cryptography, Data Security, Dual-Layer Encryption, Vigenère Cipher,

10.37802/joti.v7i1.954

Journal of Technology and Informatics (JoTI)
P-ISSN 2721-4842
E-ISSN 2686-6102
https://e-journals.dinamika.ac.id/index.php/joti

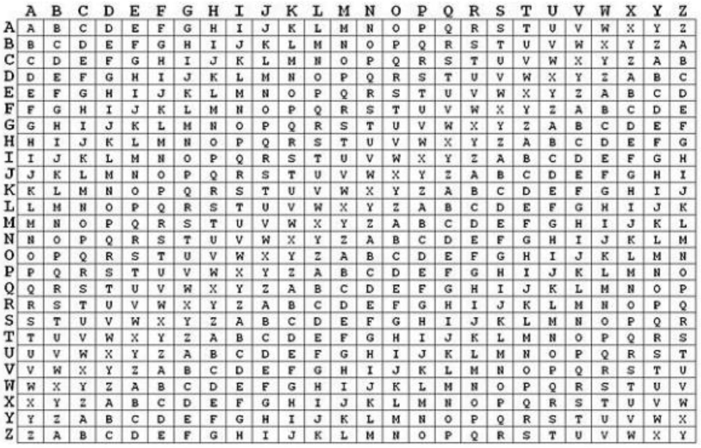
Abstract:

As technology advances further, more crimes are being committed on social media. These days, people can connect to the internet using technological devices like PCs (Personal Computers) or portable electronic devices like smartphones or tablets. This study presents a dual-layer encryption system combining the Vigenère Cipher and MySQL's AES_ENCRYPT() to enhance the security of web-based login systems. The system encrypts user credentials on the client side using the Vigenère Cipher and applies additional encryption on the server side with AES_ENCRYPT(). This approach ensures secure data transmission and storage, reducing risks of plaintext exposure and unauthorized access. Comparative testing demonstrated that the dual-layer encryption method significantly improves resistance to brute-force attacks and database breaches compared to conventional techniques like SHA-256. Encrypted credentials remain secure even in the event of a database compromise, as decryption requires the correct secret keys. The system's design also highlights the importance of robust key management to maintain data confidentiality and integrity. While this method introduces minor performance overhead and requires careful implementation, its advantages in safeguarding sensitive user information outweigh these limitations. This dual-layer approach is particularly suited for applications demanding high-security standards, making it a viable solution for mitigating contemporary cyber threats effectively.

INTRODUCTION

As technology advances further, more crimes are being committed on social media. These days, people can connect to the internet using technological devices like PCs (Personal Computers) or portable electronic devices like smartphones or tablets [1]. Different kinds of encryption are available for use. Therefore, we require a system to safeguard and stop unauthorized parties from abusing data. The encryption method is one of the strategies employed in this investigation [2]. Effective internet security is becoming more and more necessary every day. It is the responsibility of businesses to prevent the loss or theft of sensitive information. Such private information may be harmful if it is changed, lost, or ends up in the wrong hands. Therefore, they must create a plan that ensures the data will be safe from hackers. The foundation of delivering such a guarantee is cryptology [3]. The science of writing secrets is called cryptology. It consists of two components: cryptanalysis, which is the process of deciphering cryptography, and cryptography, which is the art of writing secrets. For the past 2,500 years, cryptology has developed a variety of text-hiding systems [4]. A variety of methods, referred to as cipher techniques, are employed to encode the plain text into the cipher text by utilizing an algorithm and the key [5]. The process of securely transferring data between two parties without outside interference is known as cryptography. An algorithm and a key value are used in cryptography to transform data into a format that only the participants can comprehend. The method ought to be effective and simple for the communication participants to calculate. Participants in the communication process must be able to compute the algorithm with ease and efficiency. The key is used in conjunction with the algorithm so that it can be used repeatedly with different key values. This is because it is very challenging to come up with a new algorithm each time we want to share information with someone [6].

Through the process of encryption, a message that can be understood (known as plaintext) is transformed into a code that is challenging to decipher (known as the cipher text). On the other hand, decryption is the process of converting ciphertext back into plaintext. Certain keys and mechanisms are needed for the encryption and decryption processes [7]. In this research, the encryption method that will be used is the Vigenère Cipher. This cipher uses a transferring mechanism that shifts each character in the message by a different amount. To accomplish this, a table known as the "Vigenère Table," which is a matrix with 26 rows and 26 columns, is used. The 26 language alphabets in the table are written out 26 times in multiple rows, with each letter being shifted cyclically to the left of the previous one [8].



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1. 26 x 26 Vigenère Table

The Vigenère code is a method of encoding text by replacing each character of the plain-text with another letter determined by adding of the plain text character to the index number of an arbitrarily chosen code word [3]. The Vigenère Cipher's simplicity and resistance to simple frequency analysis make it a well-liked polyalphabetic cipher. However, the key's repeated patterns are its vulnerability [9]. The encoding is often done using a table of rows of the alphabet, shifted according to the indices of the letters in the code word [4]. When the key and ciphertext are known, the plaintext will obviously also be known, making key security and distribution the crucial factors in this situation. This is among the disadvantages of algorithms that use symmetric keys [10].

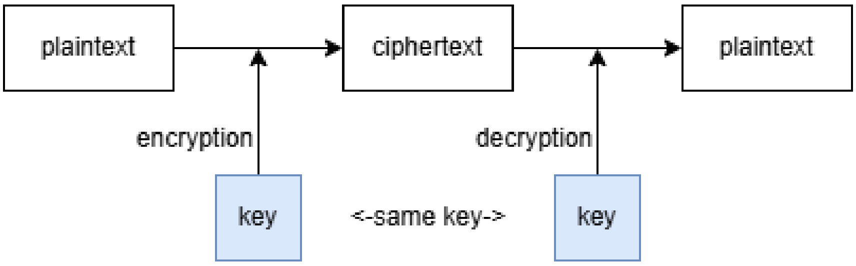


Figure 2. Symmetric Key Algorithm Scheme

An improved Vigenere cipher that is more resistant to Kasiski and Friedman assaults is required in order to get beyond the Vigenere encryption's drawbacks [11]. In order to increase the security of the Vigenère Cipher, a number of changes have been suggested. These include ways to extend the character set of ciphers to include symbols and numbers, hybrid cryptographic systems that combine Vigenère with other ciphers, and dynamic key variations [12]. Implementing a safe web-based login system that is noticeably more resistant to cyberattacks is the aim of this study. Additionally, the security and speed of this technique will be compared against more traditional approaches like SHA-256. The first step in the procedure is client-side encryption of login credentials using a modified Vigenère Cipher, which was created to improve security and fix its conventional flaws. An extra server-side encryption step is then performed using MySQL's AES_ENCRYPT() function. AES_ENCRYPT() and the enhanced Vigenère Cipher are used in this dual-layer encryption to guarantee that intercepted data is extremely safe and unintelligible.

METHOD

System Architecture

This study implements a dual-layer encryption system to secure login credentials by combining the Vigenère Cipher on the client-side and AES_ENCRYPT() on the server-side. Figure 3 illustrates the system workflow, where:

a. The user inputs their credentials (username and password) into the login form.
b. For new user registrations, the password is encrypted using the Vigenère Cipher algorithm on the client-side.
c. The encrypted password is transmitted over a secure communication protocol (e.g., HTTPS) to the server.
d. On the server-side, the AES_ENCRYPT() function is applied for additional encryption before storing the data in the database.
e. During login, the user-provided credentials are encrypted with the Vigenère Cipher and sent to the server.
f. The server retrieves the stored encrypted password and decrypts it using AES_DECRYPT().
g. The decrypted password is validated against the Vigenère-decrypted user input.
h. If the credentials match, a session is created, and the user is redirected to the dashboard; otherwise, an error message is displayed.

This workflow ensures a secure process for both storing and verifying login credentials.

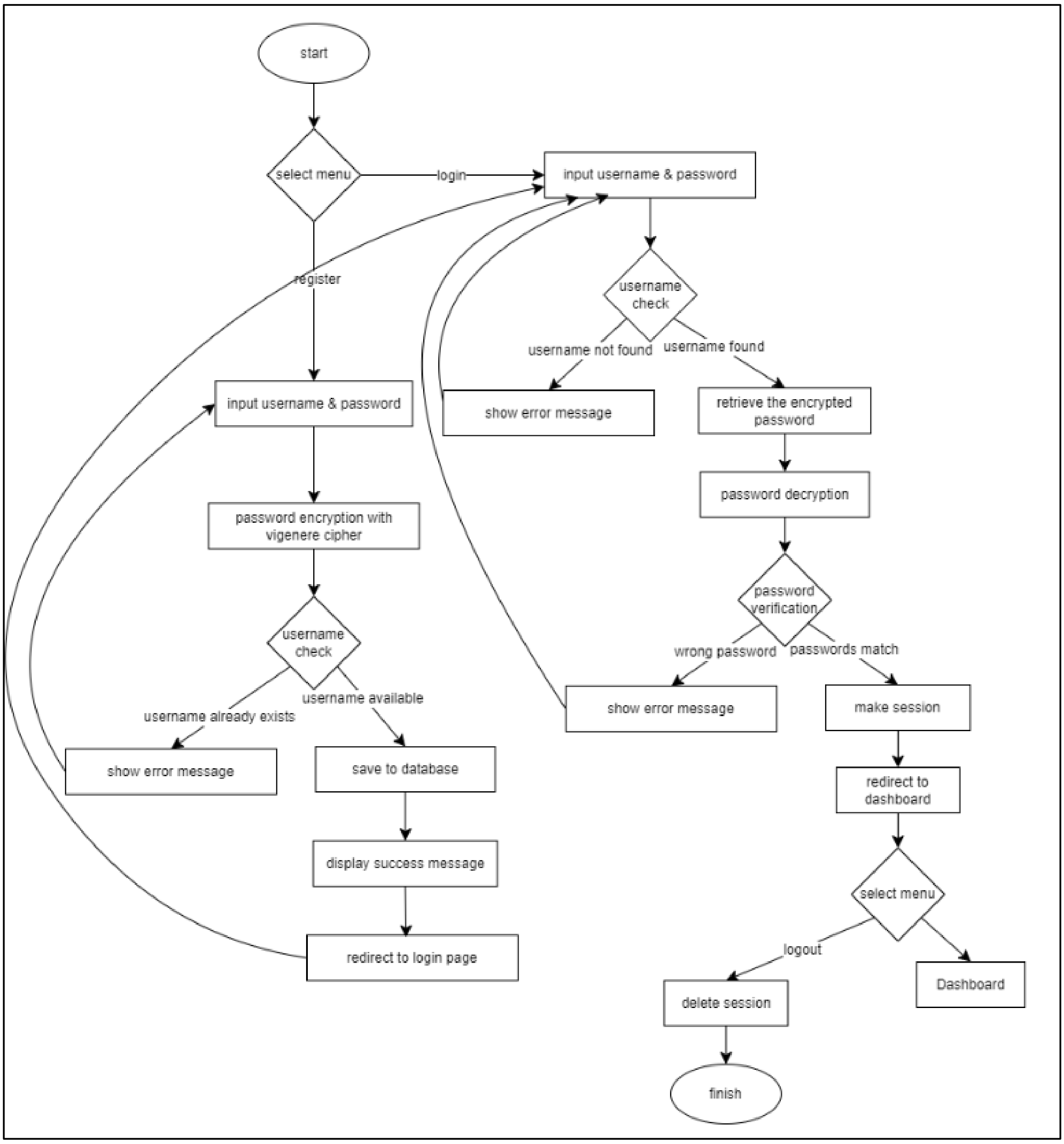


Figure 3. System Architecture Flowchart

Encryption and Decryption Process

1. *Client-Side Encryption with Vigenère Cipher*

The Vigenère Cipher is used to encrypt plaintext credentials on the client-side. The algorithm works as follows:

a. Key Selection: A predefined encryption key is chosen. This key must be securely shared between the client and server.

b. Character Substitution: Each character of the plaintext is shifted by the corresponding character in the encryption key.

c. Ciphertext Generation: The encrypted credentials are converted into ciphertext, which is then transmitted to the server.

The mathematical formula for the Vigenère Cipher is:

$$Ci = (Pi + Kj)\ mod 26 \qquad (1)$$

Where:

Ci= Encrypted character.
Pi = Plaintext character.
Kj = Corresponding key character

2. Server-Side Encryption with AES_ENCRYPT()

An additional layer of encryption is applied on the server side to enhance data security during storage. The MySQL AES_ENCRYPT() function, a symmetric encryption method renowned for its strength and effectiveness, is used in this procedure [14]. Through a combination of server-side encryption and client-side Vigenère Cipher, the system guarantees a two-layer encryption technique that protects personal information even in the event of database intrusion or interception [15]. A complete description of the procedure is provided below:

***a) Data Encryption*.**

1. Once the credentials are received by the server from the client, the data is already encrypted using the Vigenère Cipher algorithm.
2. On the server-side, this Vigenère-encrypted data undergoes further encryption using the AES_ENCRYPT() function.
3. The AES_ENCRYPT() function takes the received data and encrypts it using a predefined secret key that is securely managed on the server. This secret key is critical, as it ensures the confidentiality and integrity of the encryption process.
4. The double encryption (combining the Vigenère Cipher and AES_ENCRYPT()) ensures that the credentials are securely obfuscated, making it significantly harder for attackers to decipher even if they gain access to the data during storage or transmission.

b) Database Storage

1. The doubly-encrypted credentials are then stored securely in the database. Each entry is carefully managed to ensure that sensitive information remains protected against potential attacks, such as SQL injection or unauthorized database access.
2. The use of AES_ENCRYPT() for server-side encryption prevents the database from storing plaintext data, reducing the risk of sensitive information being exposed during a breach.

Implementation Steps

1. Key Management

a. Securely define and store the encryption key for both the Vigenère Cipher and AES_ENCRYPT().
b. Ensure restricted access to the AES secret key.\

2. Client-Side Encryption

a. Encrypt the user's plaintext credentials using the Vigenère Cipher.
b. Transmit the encrypted data securely using HTTPS.

3. Server-Side Encryption

a. Apply AES_ENCRYPT() to the received data.
b. Store the doubly-encrypted credentials in the MySQL database.

4. Login Verification

a. Decrypt stored credentials using AES_DECRYPT().
b. Compare the decrypted data with the user input.

RESULTS AND DISCUSSION

Results

The system was tested by comparing the dual-layer encryption method (Vigenère Cipher + AES_ENCRYPT()) with conventional methods such as SHA-256 hashing. The tests included scenarios like brute-force attacks and database theft simulations.

a. Resistance to Brute-Force Attacks

The combination of two encryption layers significantly increased the time required for brute-force attempts compared to single-layer methods like SHA-256. The added complexity of the Vigenère Cipher and AES_ENCRYPT() made it computationally expensive for attackers to guess the credentials.

b. Security of Stored Data

Even if the database is compromised, the data remains unreadable without the correct AES decryption key. The dual encryption ensures that credentials cannot be directly exploited by attackers.

The test results indicate that the proposed system offers a higher level of security for user credentials, particularly against common database and network-based attacks.

Table 1. Comparison of Security Methods

Methods	Brute Force Attack	Data Theft
SHA-256	Vulnerable	Vulnerable
Vigenère + AES	Secure	Secure
MD5	Vulnerable	Vulnerable

1. *Implementation of the System*

The dual-layer encryption system combining Vigenère Cipher and AES_ENCRYPT() has been successfully implemented. Below are the main components of the system:

a. Registration Page

1) Users can register by entering their username and password.
2) The data is encrypted using the Vigenère Cipher on the client-side and further encrypted with AES_ENCRYPT() on the server-side before being stored in the database.

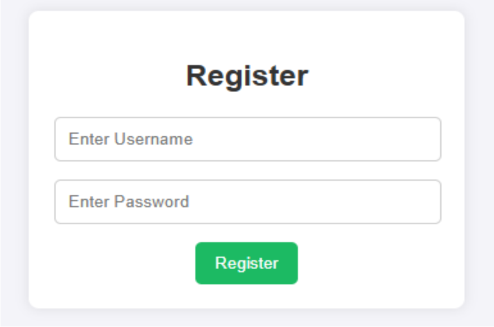
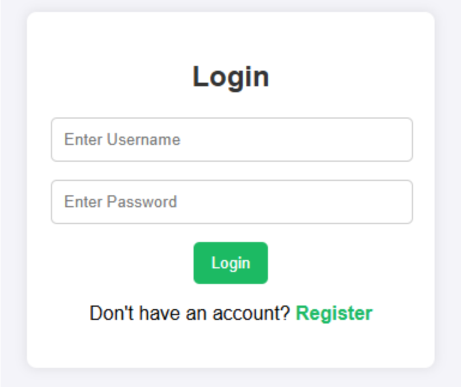


Figure 4. Registration Form

b. Login Page

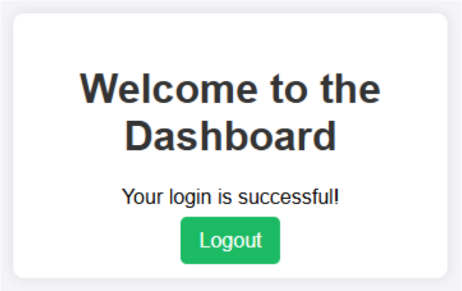
1) Users input their credentials on the login page.
2) The input is encrypted with the Vigenère Cipher and validated against the stored encrypted credentials in the database using AES_DECRYPT().



Don't have an account? Register

Figure 5. Login Form

c. Dashboard Page
Upon successful login, users are redirected to the dashboard, which confirms the validity of the entered credentials.



Welcome to the Dashboard

Your login is successful!

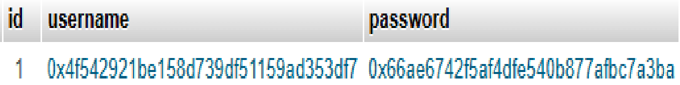
Figure 6. Dashboard Page

2. *Encryption and Decryption Process*

The system was tested using sample credentials to verify the functionality of the encryption and decryption processes. Table 2 shows the plaintext data, results after applying Vigenère Cipher and AES_ENCRYPT(), and the decrypted data during login validation.

Table 2. Encryption and Decryption Results

Plaintext	After Vigenère Cipher	After AES_ENCRYPT()	After Decryption
admin	bhlql	Encrypted Binary Data	admin
password123	rbvawskd456	Encrypted Binary Data	password123
securePass	whjlgwpih	Encrypted Binary Data	securePass



id	username	password
1	0x4f542921be158d739df51159ad353df7	0x66ae6742f5af4dfe540b877afbc7a3ba

Figure 7. Encrypted Binary Data in Database

Discussion

A significant improvement in the security of web-based login systems is provided by a two-layer encryption technique, which combines the Vigenère Cipher and AES_ENCRYPT() [16]. This approach enhances the overall security posture of the system by encrypting both the client and server [17]. By preventing plaintext data from being sent directly over the network, the Vigenère Cipher, the first layer, reduces the likelihood of transmission interception. The encrypted text produced by the Vigenère Cipher is complex enough to withstand simple cryptanalysis without a shared key, even if the data is intercepted by an attacker.

An extra layer of security is added on the server side by AES_ENCRYPT(). Data encrypted with AES_ENCRYPT() cannot be decrypted without the matching decryption key [18]. This feature is very important for maintaining the security of credentials stored in the database. Without a secret key, the encrypted data cannot be accessed even if the database is compromised, thereby significantly reducing the likelihood of data exploitation and unauthorized access. This dual-branch approach ensures strong defense against database-focused attacks such as brute-force decryption attempts or SQL injection [19].

However, this strategy is not without difficulties. Key management is one of the important components. To maintain the integrity of the system, the AES secret key needs to be stored and kept securely [20]. The entire encryption system is at risk if the key is compromised or leaked, as hackers may be able to decrypt all the stored data. To ensure long-term security, strict key management procedures are required, such as regular key rotation and secure storage options.

The performance overhead that dual-layer encryption introduces is another drawback. Although this approach greatly increases security, the encryption and decryption processes take longer to complete. Particularly in systems managing high data volumes or multiple user requests at once, users may encounter minor delays when logging in and registering. Even though the effect is usually negligible, high-performance settings where speed is essential may still encounter difficulties.

A dual-layer encryption system's implementation also necessitates meticulous preparation and execution. In contrast to single-layer techniques like SHA-256, combining two encryption algorithms adds complexity. The smooth operation of both layers requires developers to take error handling and encryption-decryption compatibility into consideration. To prevent implementation flaws or inconsistencies, sufficient testing and validation are required. Despite these drawbacks, the dual-layer encryption method offers a substantial improvement in protecting private information. It provides a well-rounded solution that successfully addresses contemporary security issues while giving data confidentiality and integrity top priority. In situations where high security standards are required, the benefits exceed the disadvantages, despite the trade-offs of increased complexity and minor performance degradation. Because of this, the method is appropriate for applications that manage sensitive user data, like financial information, login credentials, or private documents.

Future developments might concentrate on investigating cutting-edge key management systems and streamlining encryption algorithms to minimize performance overhead. The dual-layer encryption technique can develop further into a more reliable and effective way to secure web-based systems by tackling these issues.

CONCLUSIONS AND SUGGESTIONS

To improve the security of web-based login systems, this study effectively illustrated the deployment and assessment of a dual-layer encryption system that combines the Vigenère Cipher and AES_ENCRYPT(). The outcomes demonstrate how well this strategy handles important flaws in traditional techniques, like unapproved database access and plaintext exposure during transmission. The system guarantees strong data security during transmission and storage by implementing an extra encryption layer using AES_ENCRYPT() on the server-side and encrypting credentials on the client-side using the Vigenère Cipher.

According to the study, when compared to more conventional hashing techniques like SHA-256, the dual-layer encryption method greatly improves resistance to brute-force attacks and database theft. Sensitive user data is protected because, even in the event of a database breach, the encrypted credentials cannot be decrypted without the right decryption keys. For applications that demand high levels of data protection, the implementation's slight performance overhead is justified. Furthermore, the dual-layer strategy emphasizes how crucial efficient key management is. Because the AES secret key is crucial to maintaining the system's integrity, it must be securely stored and rotated on a regular basis. The system offers a scalable and secure solution for contemporary web-based systems, despite obstacles like implementation complexity and processing delays.Future research might concentrate on lowering latency in the encryption process, enhancing key management procedures, and investigating hybrid cryptographic models to further improve security. This study shows how cryptographic techniques can be combined to build robust systems that can successfully counteract modern cyberthreats.

REFERENCES

[1] V. Smith, M. Mendoza, and I. Ullah, "Data Security Techniques Using Vigenere Cipher And Steganography Methods In Inserting Text Messages In Images," vol. 3, no. 3, pp. 92–100, 2024.

[2] M. A. Putra, F. Rustan, L. M. Liwe, and K. M. Suryaningrum, "Securing Text File Using Combination of Vigenere and One - Time Pad Cipher Algorithm," *Procedia Comput. Sci.*, vol. 227, pp. 1030–1038, 2023, doi: 10.1016/j.procs.2023.10.612.

[3] S. S. Omran, A. S. Al-Khalid, and D. M. Al-Saady, "A cryptanalytic attack on Vigenère cipher using genetic algorithm," *2011 IEEE Conf. Open Syst. ICOS 2011*, no. 1, pp. 59–64, 2011, doi: 10.1109/ICOS.2011.6079312.

[4] A. Al-Sabaaw, "Cryptanalysis of Vigenère Cipher: Method Implementation," *2021 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2021*, pp. 1–4, 2021, doi: 10.1109/CSDE53843.2021.9718432.

[5] A. Saraswat, C. Khatri, Sudhakar, P. Thakral, and P. Biswas, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," *Procedia Comput. Sci.*, vol. 92, pp. 355–360, 2016, doi: 10.1016/j.procs.2016.07.390.

[6] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," *Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018*, 2018, doi: 10.1109/ICOEI.2018.8553910.

[7] B. Triandi, E. Ekadiansyah, R. Puspasari, L. T. Iwan, and F. Rahmad, "Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions," *2018 6th Int. Conf. Cyber IT Serv. Manag. CITSM 2018*, no. Citsm, pp. 1–5, 2019, doi: 10.1109/CITSM.2018.8674376.

[8] K. Nahar and P. Chakraborty, "A Modified Version of Vigenere Cipher using 95 95 Table," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 5, pp. 1144–1148, 2020, doi: 10.35940/ijeat.e9941.069520.

[9] Y. K. Singh, "Generalization of Vigenere cipher," *ARPN J. Eng. Appl. Sci.*, vol. 7, no. 1, pp. 39–44, 2012.

[10] A. Subandi, R. Meiyanti, C. L. Mestika Sandy, and R. W. Sembiring, "Three-pass protocol implementation in vigenere cipher classic cryptography algorithm with keystream generator modification," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 5, pp. 1–5, 2017, doi: 10.25046/aj020501.

[11] H. N. Abed, Z. M. Ali, and A. L. Ahmed, “A robust encryption technique using enhanced vigenère cipher,” *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 447–454, 2021, doi: 10.22075/ijnaa.2021.5071.

[12] A.-A. Mohammed and A. Olaniyan, “Vigenere Cipher: Trends, Review and Possible Modifications,” *Int. J. Comput. Appl.*, vol. 135, no. 11, pp. 46–50, 2016, doi: 10.5120/ijca2016908549.

[13] A. A. Soofi, I. Riaz, and U. Rasheed, “An Enhanced Vigenere Cipher For Data Security,” *Int. J. Sci. Technol. Res.*, vol. 5, no. 3, pp. 141–145, 2016.

[14] D. Nazelliana, “Message Security in Classical Cryptography Using the Vigenere Cipher Method,” vol. 4, no. April, pp. 350–357, 2024.

[15] R. Syahputra, “Penerapan Algoritma Vigenere Cipher Pada Aplikasi Tabungan Siswa Berbasis Web,” vol. 01, no. 06, pp. 19–23, 2024.

[16] L. Voleti, R. M. Balajee, S. K. Vallepu, K. Bayoju, and D. Srinivas, “A Secure Image Steganography Using Improved Lsb Technique and Vigenere Cipher Algorithm,” *Proc. - Int. Conf. Artif. Intell. Smart Syst. ICAIS 2021*, pp. 1005–1010, 2021, doi: 10.1109/ICAIS50930.2021.9395794.

[17] E. Irianti *et al.*, “Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa,” vol. 01, pp. 8–15, 2023.

[18] D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwan, “Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi,” vol. 3, no. 1, pp. 47–52, 2023.

[19] K. Senthil, K. Prasanthi, and R. Rajaram, “A modern avatar of Julius Ceasar and Vigenere cipher,” *2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013*, pp. 13–15, 2013, doi: 10.1109/ICCIC.2013.6724170.

[20] B. A. Buhari, R. Sulaiman, M. M. Umar, S. Shehu, A. Almu, and A. M. Abubakar, “Performance and Security Analysis of Symmetric Data Encryption Algorithms : *AES , 3DES and Blowfish*,” vol. 6486, pp. 6473–6486, 2025.