Research Article

Implementation of AES-256 Algorithm for Encryption on Chatting Platforms

[1]Saepudin Nirwan, [2*]Dini Hamidin, [3]Shifa Eldita Azzalea

[1,2,3] International University of Logistics and Business, Bandung, Indonesia

* Corresponding Author: dinihamidin@ulbi.ac.id

Abstract: This research aims to design and build a web-based corporate chat media using prototype methodology and AES (Advanced et al.) algorithm for data encryption. The platform has been developed with MERN technology (MongoDB et al.), which allows the application to be dynamic and responsive. Prototype methodology is used for iterative development based on user feedback, ensuring the application meets user needs. The AES algorithm is applied to maintain the confidentiality and security of each message sent and received. The results show that the application effectively provides efficient and secure communication for the company, with an intuitive and easy-to-use interface. Implementing MERN technology provides flexibility in the development and maintenance of the application, making it the right solution for corporate communication needs.

Keywords: Corporate Chat; Web-based; Prototype; Methodology; AES Algorithm; MERN; Data Security

Citation: Nirwan.S., et. al. (2024). Implementation of AES-256 Algorithm for Encryption on Chatting Platforms. Iota, 2024, ISSN 2774-4353, Vol.04, 04. https://doi.org/10.31763/iota.v4i4.804

Academic Editor : Adi, P.D.P

Received : September, 11 2024

Accepted : September, 24 2024

Published : November, 02 2024

1. Introduction

The rapid development of information technology has changed many aspects of life, especially in business communication in an enterprise. Companies increasingly rely on efficient, secure, and reliable communication tools to facilitate smooth employee interactions. Protecting corporate data, such as conversations and documents, is crucial to keep business information confidential and prevent potential data leakage and misuse by unauthorized parties. Corporate data often contains sensitive information such as business strategies, financial data, and employees' personal information, which, if it falls into the wrong hands, can cause significant financial and reputational damage. Data security raises demands for a better data security system to secure data from various threats that may arise (Randi et al., 2020). Data security or protection is one of the important things to protect important messages and information from corruption, compromise, or loss so that these messages and information remain safe (Wardhani & Asriningtias, 2024).

ChatCorp is a web-based communication platform designed to meet internal corporate communication needs. It provides essential features such as instant messaging, file sharing, and separate chat rooms that support efficient team collaboration. Using AES (Advanced Encryption Standard) encryption algorithm technology, ChatCorp ensures communication data security to protect corporate information from unauthorized access and theft of corporate data, such as important documents and conversations. Additional features like group chats enable real-time interactions that simplify project coordination and management. ChatCorp is specially designed with high-level security features. ChatCorp uses a prototyping approach that allows for continuous improvement based on user feedback, making it more adaptive and responsive to company needs.

In Somya's research in 2018, it can be concluded that the chat application can help EDP Finance employees or other users to communicate, attach files with a maximum size of 25 MB, and disseminate information if at any time there are additions or changes to the program developed by EDP Finance employees. The hardware and software specifications of this chat application are classified as lightweight applications because it is a web-based application; users only need a web browser to access the chat application that has been uploaded to the server, and by utilizing a local network, to access the chat application does not require an internet connection.

In the research of Muryadi et al. in 2020, the research results show that this Chatting Application can be a solution for each employee to continue to communicate, discuss, and share files between employees without having to install an application on their laptops or cellphones. This web-based chat application can be a solution to keep communicating between employees who have difficulty accessing the internet (Muryadi et al., 2020). Meanwhile, in the research of Julyanto et al. (2022), the results showed that the communication system applied the SDLC method using Caesar cipher encryption and MySQL DBMS as the database. This communication system has also been tested using black box techniques, where the system created has been tested for program functionality. The results of testing the communication system on Motor Harapan are declared valid for use (Julyanto & Deny Jollyta, 2022).

Advanced Encryption Standard (AES) is a technology used to protect confidential information in an application (Huo & Wang, 2023). ChatCorp's AES (Advanced et al.) algorithm ensures the security of conversation data and company documents. AES encrypts data using a strong encryption key so unauthorized parties cannot read it. When users send messages or documents through ChatCorp, the data is automatically encrypted before it is sent over the network. The authorized recipient uses the appropriate decryption key to restore the data to its original format. So, even if a third party intercepts the data during transmission, the third party cannot understand or use it because the data received is meaningless code without the decryption key. ChatCorp uses AES to ensure that company information is protected from potential interception and leakage and that data confidentiality and integrity are maintained at every stage of communication. AES is currently the best algorithm that provides both speed and security. It is faster than DES and Triple DES and more secure, making it the best choice for practical use (Sharma et al., 2024).

Moreover, the prototype is a software development method used to create an early version of the software, display a concept, experiment with design options, and learn more about the problem and possible solutions (Maulana et al., 2020). The prototype method allows developers to iteratively test and improve the application based on user feedback, thus ensuring that the built application can effectively meet user needs and preferences.

2. Theory

Companies need an internal communication app to ensure sensitive messages and information are kept secure and only accessed by employees. This encourages more efficient collaboration and ensures that business communications are not disrupted by security risks that may arise from using public chat apps. Companies often have highly sensitive and valuable documents and conversations, such as strategic plans, financial data, customer information, and product innovations. This information must be strictly protected so that it does not fall into the hands of unauthorized outsiders, who could use it for personal gain or to the detriment of the company. The chat application is important in a large company because it can be ascertained that one division and another division are far apart (Somya, 2018). The level of security of corporate conversations is very important because the information discussed in internal conversations often includes sensitive and strategic data. Strict protection of these conversations prevents information leakage, protects business interests, and ensures that confidential data is not misused by unauthorized parties.

2.1 Advanced Encryption Standard (AES)

Algorithm Advanced Encryption Standard (AES) is a technology used to protect confidential information in an application (Huo & Wang, 2023). Advanced Encryption Standard (AES) was introduced by Rijndael from the US National Institute of Standards and Technology competition in 2001 (Riyaldhi et al., 2017). AES has 3 categories of block ciphers: AES-128, AES-192, and AES-256 with key lengths of 128 bits, 192 bits, and 256 bits respectively. The difference between the three sequences is the key length which affects the number of rounds (Indrayani & Suartana, 2019). AES-256 Bit is a symmetric Block Cipher text that can encrypt and decrypt data/information with a key size of 256 bits (Marsiani et al., 2021).

2.2 Cryptography

Cryptography applies and studies communication and data security techniques against third parties/enemies (Marsiani et al., 2021). Based on the direction of its implementation and time divisions, cryptography can be divided into classic or conventional cryptographic algorithms and modern cryptographic algorithms (Permanasari, 2017). Classical cryptographic algorithms provide the basic concept of understanding cryptography and serve as the basis for modern cryptographic algorithms (Permanasari, 2017). The basic techniques of classical cryptographic algorithms are substitution ciphers and transposition chipers (Permanasari, 2017).

2.3 Prototype

Prototype is a basic working model for software development (Jayanti et al., 2021). The prototype method is a software development model that makes it possible not to have all the features of the final product as a whole but already has the main features and can be used to test the software before product development is complete. This method allows developers and customers to interact with each other during the project development process.

3. Method

The research method used in building the platform in this Final Project is to use Prototype Methodology or prototyping method. Prototyping methodology is an approach used in software development where a prototype or initial model of the system is created, tested, and improved based on user feedback until it reaches the final version. Using prototyping techniques when building the website for the ChatCorp website offered several significant benefits. First, this approach allows developers to better understand the needs and preferences of potential users. Second, prototyping techniques reduce the risk of project failure by identifying and fixing problems early on. Prototypes that can be tested continuously allow the development team to ensure that all features work as expected before releasing the final version. Finally, the iterative process undertaken in this methodology also allows for more flexible and responsive development. The stages carried out to compile the final project using this methodology are divided into two stages, i.e, Identification of Initial**.** Needs At this stage, the process of collecting identification of initial user needs has been carried out to develop an initial prototype of the website. In the research of Muryadi et al (2020), the need to communicate between employees is important because it can be a solution for each employee to keep communicating, discussing, and sharing files between employees without having to install an application on their laptop or cellphone (Muryadi et al., 2020). In addition, it is supported by other research by Somya (2018) saying that chat applications are important applications in a large company because it is certain that one division and another division are far apart and have difficulty communicating efficiently and quickly (Somya, 2018). And from the research that has been done, the user needs identification data obtained from the research that has been done is presented in Table 1.

Table 1. Job Analysis Table

No	Task / Job	User Needs	Description of Requirement
1	Sending Messages	Easy to use	Users should be able to send messages with an intuitive interface.
2	Receive Message	Real-time notifications	Users should be notified as soon as the message is received.
3	Managing Documents	Document Management	Users should be able to upload, download, and manage documents easily.
4	Save Communication	Data Security	Data that is transmitted and stored must be well protected.
5	Sign Up for an Account	Easy to use	The account registration process should be simple and not time-consuming.
6	Login to the App	Easy to use	The login process must be fast and secure.
7	Access various channels or rooms	Easy to use	Users should be able to easily access various channels or rooms for collaboration.

Based on the results of the job analysis table that has been done above, the user needs can be grouped in the following Table 2.

Table 2. User Needs

No	User Needs	Description
1	Data Security	Users need a strong encryption system to protect message data and documents from unauthorized access.
2	Instant messaging	Users need the ability to send and receive messages instantly with their coworkers.
3	Secure Document Sharing	Users need features for various documents with coworkers that are protected by encryption to prevent information leakage.
4	Secure User Authentication	Users need a strong authentication method (e.g.: two-factor authentication) to ensure that only authorized users can access the application.
5	Message History	Users need a feature to access message history quickly and efficiently.

This chapter includes complete coding, integration of all components, and testing to ensure that the system works properly without any issues. A successful deployment means that the system is ready to be deployed to end users. ChatCorp is a web-based chat application specifically designed for internal corporate communication. It provides essential features such as instant messaging, file sharing, and chat rooms that support team collaboration. With the integration of advanced encryption such as Advanced Encryption Standard (AES), ChatCorp ensures that all communication data remains safe and secure from unauthorized access.

3.1 Analysis of the System to be Built

In this subchapter, we will discuss and describe the flow of data transmission on the website to be built. The plan used in building this system analysis will be described in more detail in Figure 1.

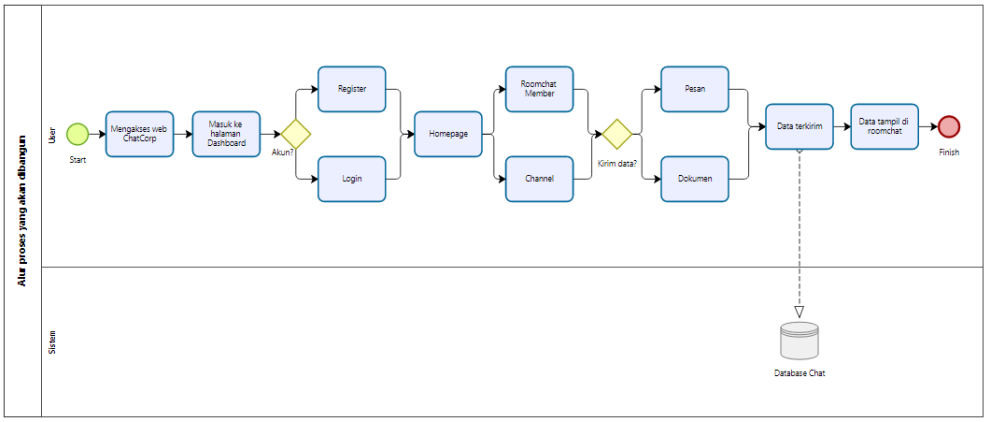

Figure 1. Block Diagram of the system to be built

3.2 Application of AES Algorithm on Chat Corp

The AES (Advanced Encryption Standard) algorithm applied to this platform is used in encrypting user conversations in the form of words, sentences, and documents that are only limited to PDF format. The encryption runs on both code files namely server.js and message.js. Equipped with a Multer that handles file uploading in web applications. Multer itself is a node.js middleware to handle form data, which is usually used to upload files.

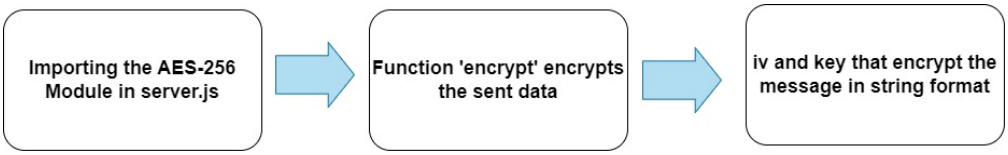

Figure 2. Flowchart of AES - 256 Algorithm Implementation

4. Result and Discussion

4.1 Experiments

Based on the implementation of the algorithm that has been carried out on the ChatCorp company chat application platform, 2 types of testing experiments were carried out, namely the first on the platform page by sending messages and checking the encryption on each message sent on the platform and starting from sending messages in the form of words, sentences, and documents that are only limited in pdf format using the black box method. Moreover, the second experiment tests how long the AES algorithm can encrypt documents in PDF format with millisecond counts using TSC (Time et al.).

4.1.1 Application Testing

The following are the steps of testing message delivery in applications encrypted by the AES (Advanced et al.) algorithm using the black box method described in Table 3.

Table 3. Test Identification Plan

No	Test Class	Test Item	Testing Level	Testing Type
1	Data security	The process of encrypting message data and documents sent by users.	Feature Testing	Blackbox Testing
2	Message Delivery	The process of sending data between users in the form of messages on the platform.	Feature Testing	Blackbox Testing
3	Berbagi Dokumen	The process of sending data between users in the form of documents in PDF format.	Feature Testing	Blackbox Testing
4	User Authentication	Process of securing data on user accounts.	Feature Testing	Blackbox Testing
5	Message History	Management of messages and documents sent by users in chat rooms.	Feature Testing	Blackbox Testing

4.1.2 Algorithm Testing

Algorithm encryption duration testing is done by calculating how long the AES algorithm takes to encrypt documents in pdf format with a size table that has been grouped into several types in Table 4.

Table 4. Pdf Document Size

No	Size Table	Size
1	Tiny	< 50 KB
2	Small	50 KB to 100 KB
3	Medium	100 KB to1 MB
4	Large	1 MB to 10 MB
5	Huge	> 10 MB

4.2 BlackBox Testing Results

BlackBox Testing Results are shown in Table 5. Table 5 concludes that the test data on data security requirements is valid because the expected data is successfully carried out and stated in the observation. Moreover, Message Delivery testing can be seen in Table 6. Table 6 concludes that the test data on the need to send messages is valid because the expected data is successfully carried out and stated in the observation. Moreover, Table 7, concludes that the test data on document-sharing requirements is valid because the expected data is successfully carried out and stated in the observation. Table 8 concludes that the test data on user authentication requirements is valid because the expected data is successfully carried out and stated in the observation.

Table 5. Data Security Testing

Data Security Testing				
Input Data	What to expect	Observation	Conclusion	
			Valid	No
Word, Sentence, Document Format pdf	Sent messages can be encrypted with a special code	Messages and documents sent on room chat are encrypted with a special code	Yes	

Table 6. Message Delivery Testing

Message Delivery Testing				
Input Data	What to expect	Observation	Conclusion	
			Valid	No
Word, Sentence	Sent messages can be displayed on the room chat page	Sent messages appear in the room chat	Yes	

Table 7. Document Sharing Testing

Testing Document sharing				
Input Data	What to expect	Observation	Conclusion	
			Valid	No
Document pdf format	Documents sent in-room chat can be displayed and accessed by other users	A document sent in room chat is displayed and accessed by other users	Yes	

Table 8. User Authentication Testing

User Authentication Testing				
Input Data	What to expect	Observation	Conclusion	
			Valid	No
Account information (name, email, password, and profile picture)	User account password information data can be secured using a special code	User account passwords are encrypted with a special code	Yes	

Table 9. Message History Testing

Message History Testing				
Input Data	What to expect	Observation	Conclusion	
			Valid	No
Words, Sentences, and pdf-formatted documents	Messages and documents sent by users can be accessed at any time	Messages and documents sent can be accessed again by the user	Yes	

Table 9 concludes that the test data on the message history requirement is valid because the expected data is successfully carried out and stated in the observation. Furthermore, Algorithm Testing Results are as follows: Encryption testing on the ChatCorp platform using TSC (Time-Stamp Counter) is done to measure the time required for the message encryption process. With TSC, measurements are made by

recording the TSC value before the encryption process begins and then recording the TSC value again after encryption is complete. The difference between these two TSC values indicates the CPU cycles required to encrypt the data. The results show how fast encryption is performed on the ChatCorp platform, which is important to ensure that encryption does not hamper application performance when used in real-time conversations. This test ensures that the platform remains responsive even when using high levels of encryption. From the experiments on the duration testing process that has been carried out, the results are described in Table 10. Table 10 shows a comparison of the time required to process a message based on its data size. This table classifies data into five categories: Tiny, Small, Medium, Large, and Huge, with size, and duration (milliseconds).

Table 10. AES Algorithm Encryption Duration Testing

No	Size Table	Size	Duration (milliseconds)
1	Tiny	< 50 KB	33.6929
2	Small	50 KB to 100 KB	31.1340
3	Medium	100 KB to1 MB	39.7492
4	Large	1 MB to 10 MB	44.0564
5	Huge	> 10 MB	38.6425

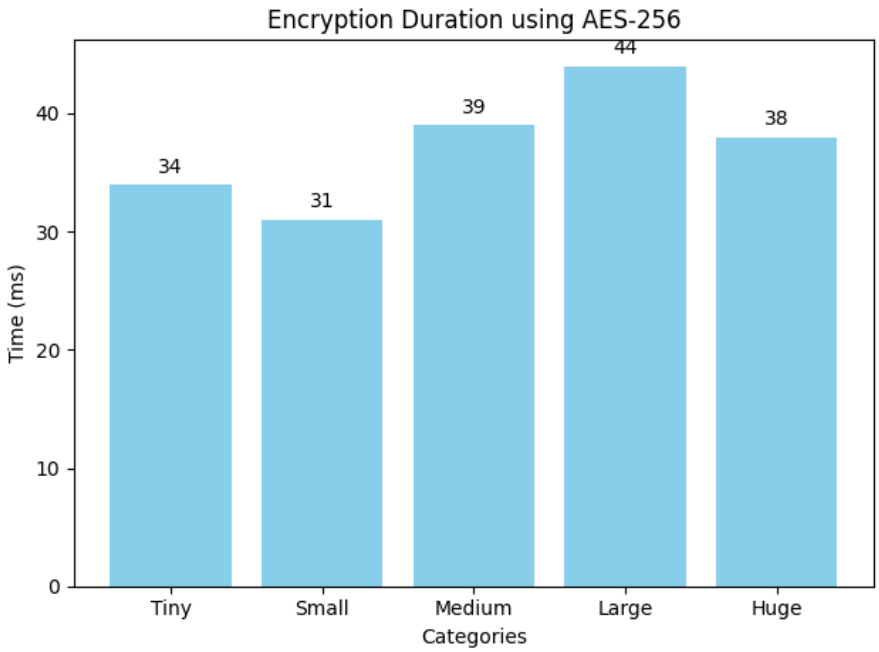

Figure 3. PDF Document Encryption Duration Chart

- The Tiny category includes data with a size below 50 kb, requiring a processing time of about 33.6929 milliseconds,
- The Small category includes data with a size of 50 kb - 100 kb, requiring a processing time of about 31.134 milliseconds,
- The Medium category includes data with a size of 100 kb - 1 mb, requiring a processing time of about 39.7492 milliseconds,
- The Large category includes data with a size of 1 mb - 10 mb, requiring a processing time of about 44.0564 milliseconds,
- The Huge category includes data with a size above 10 MB, requiring a processing time of about 38.6425 milliseconds.

Finally, Figure 3 shows that files in a small format in the graph above will take a faster duration of encryption time. As in the research conducted by Fikri et al. (2023), which states that the application can encrypt files with docx, xlxs, txt, and pdf formats, the AES-128 algorithm can be applied to population data security applications in Bogares Kidul Village; small files will be faster in the duration of encryption and decryption time.

5. Conclusion

Based on the analysis that has been done, it can be concluded that the company needs a local chat application with a high level of security that can encrypt every message and document sent by users to prevent important data leaks. The ChatCorp platform uses the AES-256-CBC algorithm to encrypt user conversations in the form of words, sentences, and PDF format documents, with the implementation of encryption running on server.js and message.js files and assisted by Multer for file uploading. Tests conducted through prototype and black box testing methods show that the messages and documents sent are successfully encrypted, ensuring that the data is safe and cannot be accessed by unauthorized parties. The platform's features, such as data security, message delivery, document sharing, user authentication, and message history, all meet the expected security and functionality standards. In addition, document encryption time is affected by file size, where small files are encrypted faster than larger files.

Acknowledgments: Thank you to all those who have supported and contributed to this research. The support and guidance from supervisors, colleagues, and family have been invaluable in completing this research. Grateful appreciation is also extended to colleagues who have provided valuable input during the research process. Hopefully, the results of this research can provide benefits and meaningful contributions to the development of science and technology.

Author contributions: All authors are responsible for building Conceptualization, Methodology, analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision of project administration, funding acquisition, and have read and agreed to the published version of the manuscript.

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

References

1. Anisa, N. (2020). Perbedaan Deployment Diagram dan Component Diagram. Sis.Binus.ac.id.
2. Dirgantara, D. A., & Andrian, R. (2023). Pengembangan Responsif Website Untuk Semarang Heritage Run 2022 dengan Framework Bootstrap. JURNAL MEDIA INFOTAMA, 19(2). https://doi.org/10.37676/jmi.v19i2.4346
3. Huo, X., & Wang, X. (2023). Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system. Results in Engineering, 20(November), 101589. https://doi.org/10.1016/j.rineng.2023.101589
4. Indrayani, L. A., & Suartana, I. M. (2019). Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document. Journal of Informatics and Computer Science (JINACS), 1(01). https://doi.org/10.26740/jinacs.v1n01.p42-47
5. Jayanti, W. E., Meilinda, E., & Fitriana, K. (2021). IMPLEMENTASI MODEL PROTOTYPE DALAM RANCANG BANGUN SISTEM INFORMASI MANAJEMEN PROYEK (SAMAR) BERBASIS WEB BAGI PERUSAHAAN KONTRAKTOR. Jurnal Informatika Kaputama (JIK), 5(1). https://doi.org/10.59697/jik.v5i1.291
6. Julyanto, & Deny Jollyta. (2022). Perancangan Aplikasi Chatting Berbasis Android Dengan Penerapan Kriptografi Menggunakan Algoritma Caesar Cipher. 4(3).
7. Marsiani, E. S., Setiadi, I., & Cahyo, A. (2021). Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi. JRKT (Jurnal Rekayasa Komputasi Terapan), 1(02). https://doi.org/10.30998/jrkt.v1i02.4096
8. Maulana, H., Kasmawi, K., & Enda, D. (2020). Buku Penghubung Berbasis Android Menggunakan Metode Prototyping. Jurnal Teknik Informatika Dan Sistem Informasi, 6(3), 521–530. https://doi.org/10.28932/jutisi.v6i3.2993
9. Muryadi, M., Zailani, A. U., & Kurniawan, Y. (2020). Rancang Bangun Aplikasi Chatting Berbasis Web Pada Pt Skemanusa Consultama Teknik. Infotech: Journal of Technology Information, 6(2), 91–100. https://doi.org/10.37365/jti.v6i2.94

10. Nabila, S., Putri, A. R., Hafizhah, A., Rahmah, F. H., & Muslikhah, R. (2021). Pemodelan Diagram UML Pada Perancangan Sistem Aplikasi Konsultasi Hewan Peliharaan Berbasis Android (Studi Kasus: Alopet). Jurnal Ilmu Komputer Dan Bisnis, 12(2), 130–139. https://doi.org/10.47927/jikb.v12i2.150
11. Nawangsih, I., & Ginanjar, E. (2019). PEMESANAN TIKET WISATA DI KABUPATEN KUNINGAN BERBASIS MOBILE. SIGMA - Jurnal Teknologi Pelita Bangsa, 10(1).
12. Novitasari, C. (2018). Pengertian Class Diagram Contoh, dan Simbolnya. In www.Pelajarindo.com.
13. Nugraha, A., Gunawan, R. D., & Ariany, F. (2023). Perancangan Sistem Marketplace Penyedia Jasa Pangkas Rambut Berbasis Website Menggunakan Mern Stack. Jurnal Ilmiah Informatika Dan Ilmu Komputer (JIMA-ILKOM), 2(2), 75–84. https://doi.org/10.58602/jima-ilkom.v2i2.20
14. Paramitha, A. (2018). Materi 4 - activity diagram. Materi 4 - Activity Diagram APSI - 2, 1(1).
15. Permanasari, Y. (2017). Kriptografi Klasik Monoalphabetic. Matematika, 16(1). https://doi.org/10.29313/jmtm.v16i1.2543
16. Pratama, A. R. (2019a). Belajar UML - Sequence Diagram - CodePolitan.com. Kodepolitan.
17. Pratama, A. R. (2019b). Belajar UML - Use Case Diagram. Codepolitan.
18. Randi, A., Lazuardy, K., Chandra, S., & Dharma, A. (2020). Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android. Jurnal Ilmu Komputer Dan Sistem Informasi, 3(2), 1–10.
19. Riyaldhi, R., Rojali, & Kurniawan, A. (2017). Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix Column. Procedia Computer Science, 116, 401–407. https://doi.org/10.1016/j.procs.2017.10.079
20. Sharma, M., Mahish, A., Singh, U. K., Chandel, R., Kumar, S., Suman, S., Isha, I., & Bhat, P. (2024). Comparative Analysis of Different Algorithms on Security of Chat Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4486950
21. Somya, R. (2018). Perancangan Aplikasi Chatting Berbasis Web di PT. Pura Barutama Kudus menggunakan Socket.IO dan Framework Foundation. Khazanah Informatika : Jurnal Ilmu Komputer Dan Informatika, 4(1), 8–15. https://doi.org/10.23917/khif.v4i1.5979
22. Sopian, Y. Y. (2018). Desain dan Implementasi Sistem Informasi Akademik (Studi Kasus STAI Sebelas April Sumedang). Infoman's, 12(2), 107–114. https://doi.org/10.33481/infomans.v12i2.158
23. Wardhani, T. D. A. P., & Asriningtias, Y. (2024). Implementasi Algoritma AES-256 Dalam Perancangan Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android. INTECOMS: Journal of Information Technology and Computer Science, 6(2), 1289–1293. https://doi.org/10.31539/intecoms.v6i2.8027