Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

SECURED CHAT-API WITH E2EE TECHNIQUES AND WEBSITE ANALYSIS USING PERFORMANCE MONITORING SOFTWARE

Nur Izzatul Aqma Zulkarnain and Abidah Haji Mat Taib
College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
niazaqma25@gmail.com and abidah@uitm.edu.my

ABSTRACT – Secured website chat has been a great approach to interact with potential new clients and provide users the assurance required to communicate through the business. A secure chat API using E2EE techniques and Telegram API ensures high level security and privacy. AES-256 encryption provides efficient and fast encryption and decryption processes, enabling smooth communication. Performance monitoring by Super Monitoring and Google extension ensures impressive results. THis secure chat API website provides a secure and efficient platform for private communication.

Keywords: E2EE, AES-256, RSA, SuperMonitoring, loading time, response time, recovery time

1. INTRODUCTION

This study enhanced the use of E2EE techniques in Telegram API. The developed website will be added with a chat feature that can be directly sent to the recipient through Telegram-API that has been invoked into group chat. The encrypted information transmitted through the website chat is stored inside a database, MySQL. Then, the information went through decryption and sent through the Telegram API towards the recipient. The algorithm used in the encryption is AES-256 and RSA which has the highest rank of secured algorithm. The reason for using two algorithms is to compare the analysis result at the end of the project testing. The implementation of AES-256 algorithms is the final security measurement will be installed in this website chat along with a URL filter attached to the chat feature to filter any malicious link attached by the sender.

2. METHODOLOGY

The methods involved in this study are collecting data from the client regarding the need of secured website chat and implementing E2EE techniques which are AES-256 algorithms to encrypt the data sent by the client. Script writing is in Visual Code studio and openssl installer is used to get the encryption key for both AES-256 and RSA algorithms. The analysis results are compared using performance monitoring software attached with the website's URL.

2.1 System Design

The system is simply built with an interface using HTML language with several information regarding the sender and sent through Telegram-API towards the recipient. The information transmitted is encrypted and stored in a MySQL database. Then, the information is decrypted with the encryption key and sent to the recipient Telegram account. The message sent by the sender will go through the URL filter if there is any URL detected attached to the message sent to ensure the recipient does not click on any malicious link.

3. RESULTS AND DISCUSSION

In this context, the result of loading time, response and recovery time based on different browser pages using monitoring software show that AES-256 algorithm implementation is better than RSA algorithm implementation due to less work on converting the keys for encryption and less scripting load when executed.

The results show the lab and field data retrieved from monitoring software called SuperMonitoring for two different implementations between RSA and AES-256 on website chat. Hence, the comparison between RSA and AES-256 in terms of loading, recovery, and response time are made according to the results report.

Table 1. Analysis result comparison for both algorithms

Components	AES-256	RSA
Average response time	Min. value: 0 min (number of events = 3) Max. value: 0 min (number of events = 9)	Min. value: 0 min (number of events = 1) Max. value: 0 min (number of events = 3)
Average loading time	Min. value: 3.53s Max. value: 9.89s	Min. value: 4.93 Max. value: 11.6s
Average recovery time (RTO)	28.544%	35.728%
Uptime% - downtime%		

The best number of events executed per 0 minute should be 0 minute per 15 events (Sharma, 2020), however, the nearest result obtained should be AES-256 algorithm average response time which is 0 minute 9 events.

4. NOVELTY OF RESEARCH / PRODUCT

Our research project focuses on developing a highly secured chat API using AES-256 encryption. This project aims to address the concerns of privacy and data security in online communication platforms. By implementing AES-256 encryption, which is widely regarded as one of the most secure encryption algorithms, we aim to provide users with a secure and private chat experience. This research project will contribute to the field by developing an efficient chat chat API that ensures end-to-end encryption, preventing unauthorized access to sensitive user data.

5. CONCLUSION

Overall, the project has achieved its objective of developing secured chat-API for developed website chat and exploring hybrid cryptography to increase security, expand database sizes to store more encrypted data, incorporating new features such as automatic generating of encryption keys.

REFERENCES

Bogos C. E., Mocanu R., Simion E. (2023). A security analysis comparison between Signal, WhatsApp and Telegram. *Journal of Applied Science, 11, 7783. https://doi.org/10/3391/app11172799*

Verma R., Sharma A. K. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications,Vol 11,4.* http://dx.doi.org/10.29322/IJSRP.10.04.2020.p10013

Multi G.W.W., & Setiawan H. (2020). Designing and Building Secure Electronic Medical Record Application by Applying AES-256 and RSA Digital Signature. *IOP Conf. Ser.: Mater. Sci. End. 852 012148*