UDC 004.7

WEB-BASED CRYPTOGRAPHIC MESSAGING SYSTEM

Clinton Chukwuemeka Clinton[1], Yurii Maslyiak[2]
West Ukrainian National University
[1] Master's Degree student, [2] PhD., Lecturer

I. Formulation of the problem

In this era of technology, there a lot of attempts by hackers to exploit weakness in computer systems or computer networks [1-4]. This is why sending and receiving of the information must be secure and safe. To ensure this, cryptography is used. If hacker will eventually breaks into the network or server hewill only see the encrypted messages which will be impossible or will take a whole lot of time to decipher, which by then those messages or information would have been rendered useless or invalid.

II. The purpose of the work

The purpose of the research is to develop a web-based cryptographic messaging system for transferring encrypted data over a network in a secure way.

III. Software implementation

The software has been created using advanced encryption standard (AES) algorithm. It is been used to encrypt messages before been sent over a network. AES is a symmetric encryption algorithm.It means that both the sender and the receiver use the same key for both encryption and decryption[1].

Packet analyzer like Wireshark has been used to ensure that the sent data was encrypted and unable to understood by a third-party. Another feature software feature is storing messages in encrypted format with expiry timestamp, should eventually the database be compromised, the hacker would only see encrypted messages or an empty database.

The use case diagramdepicts the actors (persons who have access to the functions of the program) and the functions of the software product themselves (see fig.1).

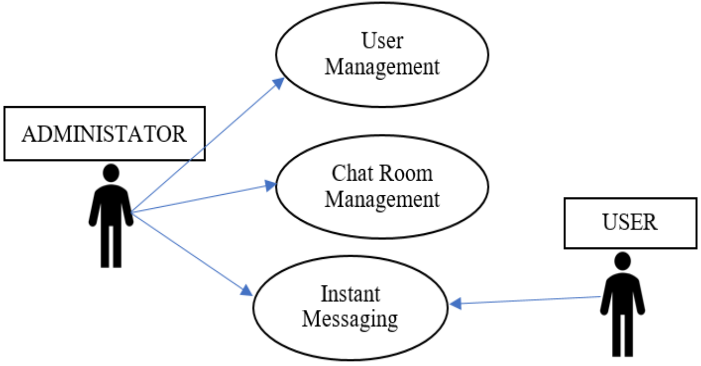

Figure 1 – Use case diagram of the developed software for cryptographic messaging system

React.js, Node.js and MongoDB have been used to implement the software.

Conclusion

The creation of a safe and fastmeans of communication between users in an organization has been the main focus of this research since inception. This idea was conceived to create a safe system to help organizations which deal with sensitive data transfer among the users.

Reference

1. T. Point "Advanced Encryption Standard" 13 October 2020. [Online] – Access mode: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm.
2. Коркішко Т. Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSec / Т. Коркішко, Л. Коркішко, Р. Шевчук // Комп'ютинг. – 2003. – Т. 2, No 1. – С. 41–47.
3. Ivasiev, M. Kasianchuk, I. Yakymenko, R. Shevchuk, M. Karpinski and O. Gomotiuk, "Effective Algorithms for Finding the Remainder of Multi-Digit Numbers", 2019 9th International Conference on Advanced Computer Information Technologies, Jun. 2019.
4. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The Method of Factorizing Multi-Digit Numbers Based on the Operation of Adding Odd Numbers. Proceedings of the conference «Advanced Computer Information Technology (ACIT 2018)» (Ceske Budejovice, Czech Republic). P. 232–235