INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 2319-2321

HIGHLY EFFICIENT AND RE-EXECUTABLE PRIVATE FUNCTION EVALUATION WITH LINEAR COMPLEXITY

G. Jidhush[1], Dr. K. Srinivasan[2]

[1]PG Scholar, Department of Computer Science and Applications, SCSVMV [Deemed to be University], Kanchipuram, Tamil Nadu, India.

[2]Assistant Professor, Department of Computer Science and Applications, SCSVMV [Deemed to be University], Kanchipuram, Tamil Nadu, India.

ABSTRACT

This project is based on the cryptography security system. Here we will be using the encryption and decryption using the email authentication code for security purpose. The encryption process involves converting the plaintext message into a series of characters based on an email code, which comprises a combination of alphanumeric characters and special symbols. This email code is generated using a key that is known only to the sender and recipient, ensuring the confidentiality of the message. The plaintext message is transformed into ciphertext by replacing each character with its corresponding email code representation. The decryption process requires the recipient to possess the same key as the sender. By reversing the encryption algorithm, the recipient can convert the ciphertext back into plaintext, thus retrieving the original message. The email code acts as a crucial component in ensuring secure communication, as it adds an additional layer of complexity to the encryption and decryption processes.

Keywords: Secure Computing, Fernet Algorithm.

1. INTRODUCTION

This project is based on the cryptography security system. Here we will be using the encryption and decryption using the email authentication code for security purpose. The encryption process involves converting the plaintext message into a series of characters based on an email code, which comprises a combination of alphanumeric characters and special symbols. This email code is generated using a key that is known only to the sender and recipient, ensuring the confidentiality of the message. The plaintext message is transformed into ciphertext by replacing each character with its corresponding email code representation. The decryption process requires the recipient to possess the same key as the sender.

2. LITERATURE SURVEY

1. A. Paus, A.-R. Sadeghi, and T. Schneider, was presented at the ACNS (Applied Cryptography and Network Security) conference in 2009. This conference is a prominent venue for presenting research in the field of cryptography and network security.
2. J. Katz and L. Malka, presented at ASIACRYPT 2011, seems to address the efficient evaluation of private functions while maintaining constant communication rounds and linear complexity.
3. P. Mohassel and S. Sadeghian, presented at EUROCRYPT 2013, appears to focus on enhancing the efficiency of secure multi-party computation (MPC) protocols by hiding the underlying circuits used for computation.
4. M. A. Bingol, O. Bic¸er, M. S. Kiraz, and A. Levi, published in the Computer Journal in 2019, presents a protocol for performing private function evaluation between two parties efficiently using half gates.
5. A. Kiss and T. Schneider, presented at EUROCRYPT 2016, likely focuses on practical aspects of Valiant's universal circuit construction, a significant development in the field of secure computation.

3. OBJECTIVES

Comparative analysis of nutrient compositions in aeroponically and soil-cultivated crops. Rigorous sampling and analytical techniques employed for quantitative data collection. Holistic approach to understanding overall nutritional dynamics, avoiding explicit mention of individual nutrients.

4. PROPOSED SYSTEM

As our proposed system deals with the system which uses email code for security keys to provide strong two-factor authentication and secure encryption and decryption of data. These keys are designed to prevent phishing and other types of attacks, making them highly secure. The system will include a user management system that allows administrators to manage user accounts. Users register with the system and generate a pair of encryption keys, including a public key for encryption and a private key for decryption. These keys are securely stored on the user's

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 2319-2321

device. When composing an email, the sender selects the option to encrypt the message.

CLASS DIAGRAM

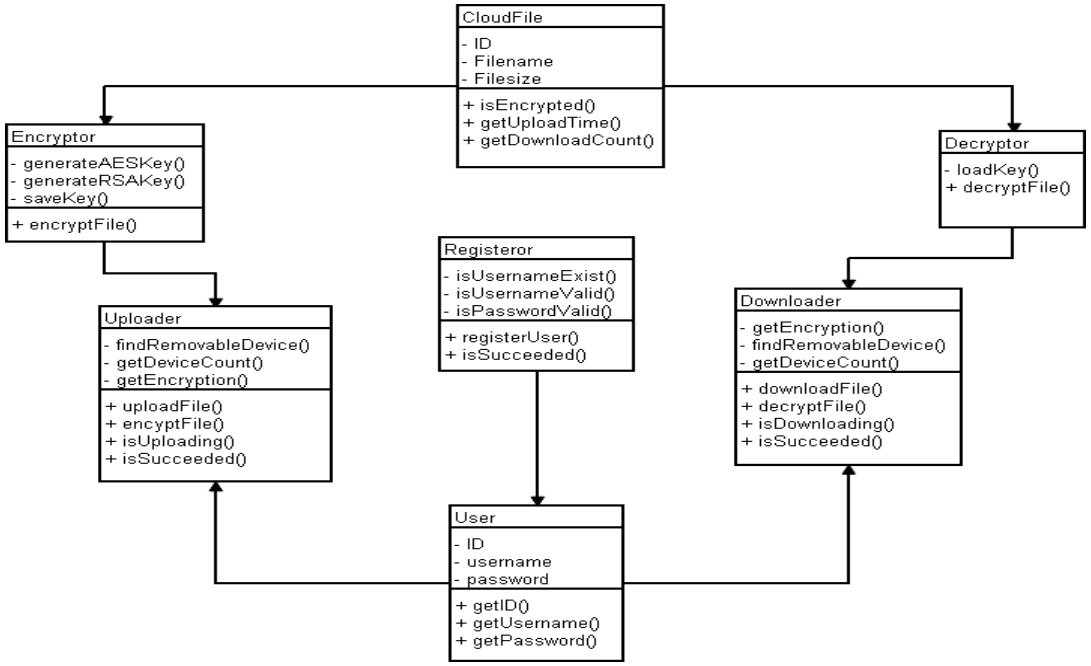

Figure 1: Class Diagram: Shows the classes and their relationships in the system design. Provides a structural view of the systems architecture

5. SYSTEM ARCHITECTURE

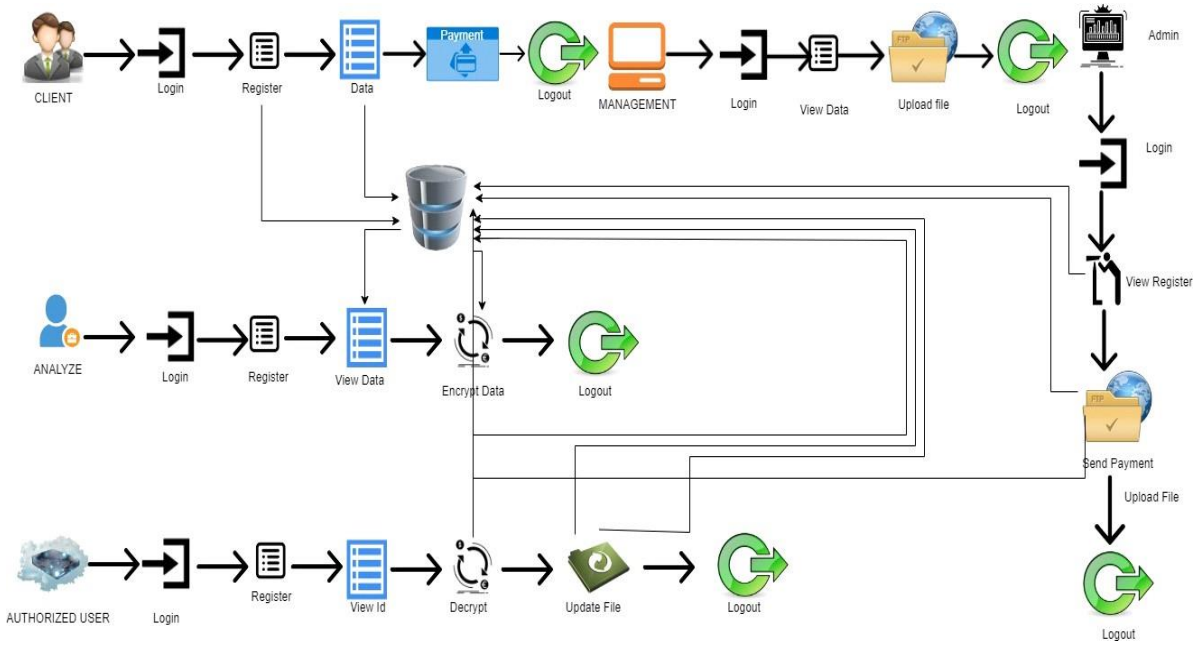

Figure 2: System Architecture : Illustrates the overall architecture and flow of the system.

6. CONCLUSION AND FUTURE WORKS

The addresses key aspects such as key generation and management encryption and decryption processes, key exchange, authentication, and integrity verification. It integrates seamlessly into popular email clients or can be implemented as a standalone application, providing a user-friendly interface for enabling encryption and decryption functionalities. With its emphasis on scalability and performance, the system can handle a large number of users and email traffic efficiently, ensuring timely and reliable encryption and decryption operations. Overall, the encryption and decryption system using email code for cryptography combines the convenience of email communication with robust cryptographic techniques, providing users with a secure and user-friendly method for protecting sensitive information transmitted via email. This is to protect the sensitive data and to protect the users from hackers.

7. REFERENCES

[1] A. Paus, A.-R. Sadeghi, and T. Schneider, "Practical secure evaluation of semi-private functions," in ACNS 2009. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 89– 106.

[2] J. Katz and L. Malka, "Constant-round private function evaluation with linear complexity," in ASIACRYPT 2011, Seoul, South Korea, December 4-8, Berlin, Heidelberg,

[3] 2011, pp. 556–571

[4] P. Mohassel and S. Sadeghian, "How to hide circuits in mpc an efficient framework for private function evaluation," in Advances in Cryptology – EUROCRYPT 2013, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, vol. 7881, pp. 557–574.

[5] S. Sadeghian, "New Techniques for Private Function Evaluation," Ph.D. dissertation, University of Calgary, 2015.

[6] M. A. Bingol, O. Bic ¸er, M. S. Kiraz, and A. Levi, "An efficient 2-party private function evaluation protocol based on half gates," Compute. J., vol. 62, no. 4, pp. 598–613, 2019. [Online]. Available: https://doi.org/10.1093/comjnl/bxy136