IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 6, Issue 1, June 2021
Impact Factor: 4.819

Implementation of Hybrid Cryptography on Cloud

Aishwarya Nawal[1], Harish Soni[2], Shweta Arewar[3], Varshita Gangadhara[4]
Students, Department of Computer Engineering[1,2,3,4]
Sinhgad Institute of Technology, Lonavala, India

I. INTRODUCTION

The cloud storage enables you to store your data on hosted servers. When the different organizations use the cloud to store their data, there is often a risk of data misuse. To avoid this type of risk, there is an imminent need to secure the data repositories. Since, sensitive data is present on the cloud there is a need to protect this data from Unauthorized Access. This Security concern of protecting the data from unauthorized access can be solved using various ways, the most commonly used techniques are cryptography. The software product is liable to meet the required security needs of data centre of cloud. AES-GCM used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The idea of splitting files and merging files on to meet the principle of data security. The hybrid approach when deployed to the cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. Cryptography technique translates the original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate the data into unreadable form. So only authorized person can have access data from cloud server. Cipher text data is visible for all people.

II. PROBLEM STATEMENT AND OBJECTIVE

The amount of data being stored in the cloud is increasing daily and there is a need to provide more than a basic level of security to the data stored and also to be shared. Thus, there is a need for such a system that will provide security to the data through cryptography. The system for encryption and decryption must be both strong and within the scope of implementation. For this, Hybrid cryptography is implemented.

1. The amount of stored data on the internet become larger and larger every day.
2. There is need of an encryption algorithm that guarantee Security of data
3. This research paper presents a model for encrypting cloud data.
4. We use Hybrid Cryptography to tackle this problem and provide secure storage on cloud

2.1 Objectives

1. To achieve secure file storage on the cloud using hybrid cryptography.
2. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled.

III. LITERATURE SURVEY

The paper titled Packed AES-GCM Algorithm Suitable for AES/PCLMULQDQ Instructions published in IEEE Computer Society in March 2011.The authors Krzysztof Jankowski and Pierre Laurent suggested that in the last few years the level of interest in Galois Counter Mode (GCM) Authenticated Encryption rose significantly. GCM is interesting because it is the only authenticated encryption standard that can be implemented in a fully pipelined or parallelized way and it is the most appropriate for encrypting packetized data. The implementation strategy have a broader appeal, which makes this optimization can be used even when there is a single multiplier. Packed AES-GCM implementation proposed in this paper proved to be very efficient. However, further optimizations are possible and are under investigation. And Challenges in this paper is faster instructions count. And key points are Software, data encryption, AES, GCM, performance evaluation of algorithms.

The paper titled Hybrid Cryptography WAKE(Word Auto Key Encryption)and Binary Casear Method For Data Security published at 6th International Conference on Cyber and IT Service Management 2018. The authors Mikha

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 6, Issue 1, June 2021
Impact Factor: 4.819

Dayan Sinaga ,Nita Sari Br Sembiring, Frinto Tambunan and Charles Jhony Mantho Sianturisuggested that the general idea about how file encryption and decryption is implemented using cryptography technique. Security of data or documents is vital issue nowadays. In simple ways, the goal is to make data unreadable by a third party. Hence a secure system should maintain the integrity, availability and privacy of data. Data integrity usually means protection from unauthorized modification and protection from undetected modification. Cryptography is grouped into symmetric key and asymmetric key. In symmetric cryptography, encrypted and decrypted key are the same. And in contrast, cryptography using different encrypted keys from decrypted key is called asymmetric cryptography. Because of its characteristics the asymmetric is more secure than symmetric but symmetric cryptography is significantly faster than asymmetric. Hence, we are using symmetric key. In general cryptography has four main components: Plaintext, Cipher text, key and Algorithm.

The paper titled An Efficient FPGA Implementation of AES-CCM Authenticated Encryption IP Core published at 2016 IEEE 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science. The authors Thi-Thanh-Dung Phan, Van-Phuc Hoang and Van-Lan Dao suggested that the implementation results on FGPA show that the protocol AES-CCM core has higher resource usage efficiency as compared with other designs. Recently, wireless networks are developed more and more so that they provide a wide range of applications and connectivity. The authors also summarized some main security requirements and introduced some techniques to protect the system from possible attacks by several modes of operations such as encryption only.But more improvements were desired since emerging wireless body area networks require low area, ultra-low power consumption encrypted authentication cores. Therefore, this work focuses on the FGPA implementation of a low area AES-CCM IP Core to provide both message encryption and authentication requirements. This study proves that by using AES-CCM algorithm you can encrypt the data efficiently without causing any harm to the concerned security issues. The drawback of this paper was the proposed AES-CCM IP Core could not be implemented on ASIC hardware platform hence it did not fulfil the resource and power constraint application.

The paper titled ChaCha20-Poly1305 Authenticated Encryption for High-Speed Embedded IoT Applications published at 2017 IEEE. The authors Fabrizio De Santis, Andreas Schauer, and Georg Sigl suggested that ChaCha20-Poly1305 Authenticated Encryption for High-Speed Embedded IoT Applications: The ChaCha20 stream cipher and the Poly1305 authenticator are cryptographic algorithms designed by Daniel J. Bernstein with the aim of ensuring high-security margins, while achieving high performance on a broad range of software platforms.

The paper titled Hybrid Cryptography Algorithms in Cloud Computing: A Review published in IEEE Xplore on 23 March 2020,15th International Conference on Electronics Computer and Computation (ICECCO 2019).The authors Sadiq Aliyu Ahmad, Ahmed Baita Garko suggested that , a study of hybrid cryptography has been performed from 2015 to early 2019. Papers related to the problem of cloud security were searched and about 20 were considered. Of these, eight are based on a user-friendly tabular survey and 12 are in-depth surveys. The main aim of this review paper is to provide more knowledge to people wanting to understand and implemented cloud security using hybrid cryptography. The research gap identified are both user authentication and practical application of the model suggested by the researchers.

IV. ALGORITHM PROPOSED

For Encryption :

- Step 1: Load the file on the server.
- Step 2: Divide the given file into N parts.
- Step 3: Encrypting all the parts of the file using any one of the selected algorithms.
- Step 4: The keys for cryptography algorithms is then secured using one of the selected algorithm.

For Decryption:

- Step 1: Load the key on the server.
- Step 2: Decrypt the keys of the algorithms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 6, Issue 1, June 2021
Impact Factor: 4.819

- Step 3: Decrypt all the N parts of the file using the same algorithms which were used to encrypt them.
- Step 4: Combining all the N parts to form the original file and provide it to the user for downloading.

Below is the System Architecture it shows the systematic flow of how the file is been divided into N parts then how it is encrypted and decrypted on cloud and then finally accessed.

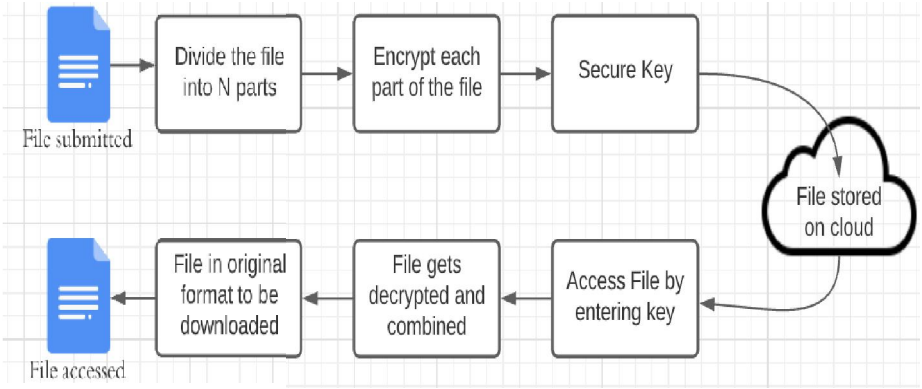

Figure 1: System Architecture

Here is the Activity Diagram showing the flow of system.

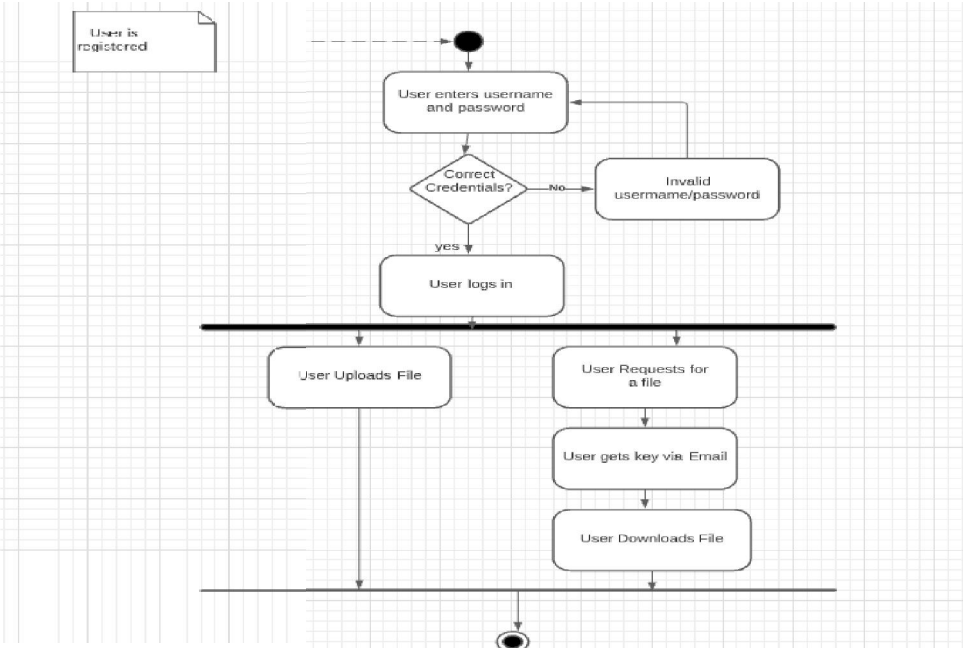

Figure 2: Activity Diagram

V. Overview of Proposed System

5.1 Hardware used in our System

- Minimum 2 GB RAM
- Hard Disk Space-500 MB

5.2 Software used in our System

- This software is developed using python, HTML, CSS and Java script and AWS cloud server.
- Python IDE, XAMPP, Sublime Text3, AWS console account

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 6, Issue 1, June 2021
Impact Factor: 4.819

5.3 Database used in our System

- The database is the cloud server.
- Here, we have used an Amazon Web Services.

VI. TESTING RESULTS

Manual testing- The test cases are executed manually by a tester without using any automated tools is termed as **manual testing which** is a type of software testing. To identify the bugs, issues, and defects in the software application is main purpose of Manual Testing. This testing helps to find critical bugs in the software application as Manual software testing is the most primitive technique of all testing types. So here we have done manual testing for our system. Below is the Test cases & Test Results of our system.

6.1 Registration User Module

SR. NO	Test Case	Excepted Result	Test Result
1	At first user have to fill all fields with proper data, enter username, password, email then it gives proper message otherwise user record is not adding to the Database.	Software should display main window	Successfully

6.2 Login User Module

SR. NO	Test Case	Excepted Result	Test Result
1	Enter valid username and password & click on login button	Software should display main window	Successfully
2	Enter invalid	Software should not display main window	successfully

6.3 Upload File Module

SR.NO	Test Case	Excepted Result	Test Result
1	Upload the file	Software should display main window	Successfully

6.4 Download File Module

SR.NO	Test Case	Excepted Result	Test Result
1	Enter valid key and click on download file	Software should display main window	successfully
2	Enter invalid	Software should not display main window	successfully

6.5 Results

1. Secure files can be accessed only to the authorised person
2. Files are stored in encrypted format using Hybrid Cryptography
3. Alert message will be sent if invalid key detection happened.

The Screenshots of our outcomes are given below:

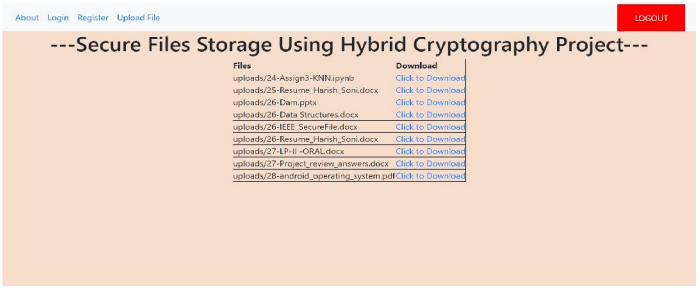

Figure 1: This page includes the files uploaded on our system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 6, Issue 1, June 2021
Impact Factor: 4.819

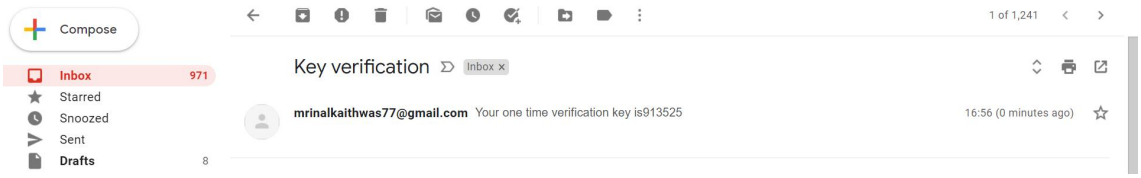

Figure 2: The key verification sent through E-mail.

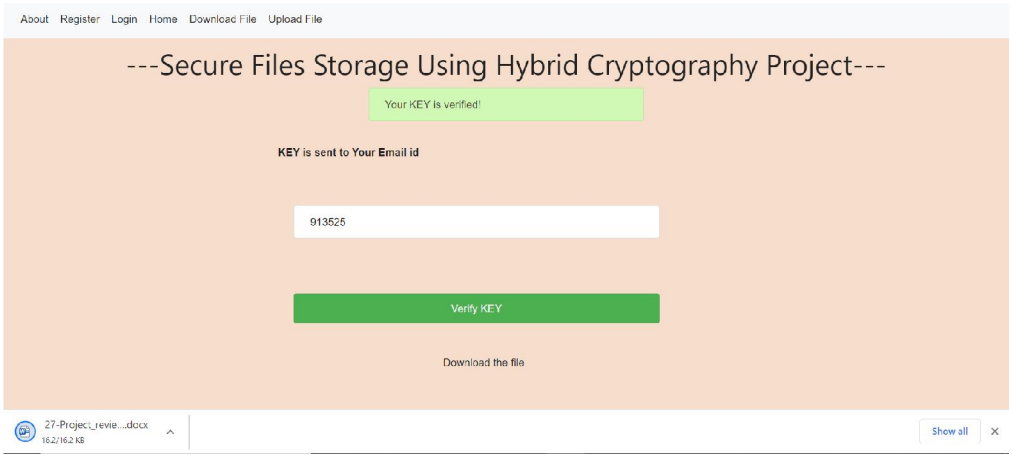

Figure 3 : End result where file is been downloaded

VII. Comparison Study

Comparison study between our system and the existing systems:

This comparison study is done based on one of our reference papers namely: Hybrid Cryptography Algorithms in Cloud Computing: A Review. In this paper, a study of hybrid cryptography has been performed from 2015 to early 2019. We will be comparing the system that we have implemented to the existing systems presented in the paper. Our system is a combination of symmetric key cryptography algorithms namely AES-GCM, AES-CCM, FERNET, and CHACHA20-POLY1305. Our system divides the file during encryption and combines it during decryption. The symmetric algorithms have the advantage of low data delay when it comes to encryption and decryption. These algorithms are virtually impenetrable using brute-force methods. Whenever a system, used an asymmetric key cryptography algorithm the time taken for the encryption-decryption process was comparatively high as these algorithms use longer keys. We have not used any of the algorithms such as MD5 which is now considered not to be secure anymore. Here, user authentication is not neglected. We have provided a platform for the user to login and register and if failed to do so three times, they will be sent an alert on their email id. Also, the user cannot download any file without the consent of the owner of the file which increases the security further. Unlike the systems talked about in the paper, the physical implementation of our system is done. The implementation is in no way neglected. The two problems highlighted by the authors in the paper were thought of and put as a requirement for our system. Our system has future scope for the security of both image and video files.

VIII. Conclusion

Cloud can handle the future requirements of accessing multimedia files because of limited capabilities of low configured devices available. But the cloud and its users have many privacy and security related aspects that requires special attention. Data security and privacy protection are the primary problems that need to be solved. The model proposed here is a secure hybrid cryptography approach scenario to provide a safe storage and safe transmission for Confidential Data files.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 6, Issue 1, June 2021
Impact Factor: 4.819

ACKNOWLEDGMENT

I am extremely grateful to, Principal Sinhgad Institute of Technology and Head of Department, Department of Computer Science for providing all the required resources for the successful completion of my project. My heartful gratitude to my project guide Dr. S. D. Babar, Department of Computer Science for valuable suggestions and guidance in the preparation of the report. I express my thanks to the authors of the references and other works of literature referred to in the project.

REFERENCES

[1] Jankowski, K., & Laurent, P. (2011). Packed AES-GCM Algorithm Suitable for AES/PCLMULQDQ Instructions. IEEE Transactions on Computers, 60(1), 135–138. doi:10.1109/tc.2010.147.

[2] Sinaga, M. D., Sembiring, N. S. B., Tambunan, F., &Sianturi, C. J. M. (2018). Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method For Data Security. 2018 6th International Conference on Cyber and IT Service Management (CITSM). doi:10.1109/citsm.2018.8674346.

[3] Phan, T.-T.-D., Hoang, V.-P., & Dao, V.-L. (2016). An efficient FPGA implementation of AES-CCM authenticated encryption IP core. 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS). doi:10.1109/nics.2016.7725650.

[4] De Santis, F., Schauer, A., &Sigl, G. (2017). ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. doi:10.23919/date.2017.7927078.

[5] Ahmad, S. A., &Garko, A. B. (2019). Hybrid Cryptography Algorithms in Cloud Computing: A Review. 2019 15th International Conference on Electronics, Computer and Computation (ICECCO). doi:10.1109/icecco48375.2019.9043254.

[6] K. Jasleen and S. Garg, "Security in Cloud Computing using Hybrid of Algorithms", IJERJS, vol. 3, no. 5, pp. 300-305, September-October 2015, ISSN 2091-2730