International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I9P237
Volume 70 Issue 9, 371-375, September 2022

Original Article

Cloud Storage Security using Firebase and Fernet Encryption

Dhruv Sharma[1], C. Fancy[2]

[1,2]*Department of Networking and Communication, SRM Institute of Science and Technology, Tamilnadu, India.*

[2]*Corresponding Author : fancyc@srmist.edu.in*

Received: 12 May 2022 Revised: 14 July 2022 Accepted: 19 September 2022 Published: 30 September 2022

Abstract *- In a brief span of time, cloud computing has revolutionized from a small network of computers to virtualizing 'n' a number of operating systems on your personal system. It offers a lot of services in just one click. The services are majorly divided into three categories, Infrastructure as a service (IAAS), Platform as a service (PAAS) and Software as a Service (SAAS). There are all possible measures taken to make the cloud secure to work in. They are services-level agreements to clearly explain the security of the clouds and security in the cloud. One of the best and most acceptable methods to secure the data in the cloud is through Encryption Techniques. Encryption Techniques are different for data in rest and data in transition. Still, the probability of data breaches in the cloud has increased from 27.9 percent in 2018 to 29.6 percent in 2019. All confidential and sensitive data falls in the hand of the attacker, which might damage the organization's reputation. Adding an extra layer of encryption, data can be secured. If, in some way or the other, the data fall into the wrong hands, even in that condition, the attacker will not be able to open the data as it has double protection and a doubly encrypted layer. So, to add this extra layer of encryption, there are multiple techniques. Some of the most used are DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA (Rivest, Shamir and Adleman) and Blowfish algorithm.*

Keywords *- Cloud computing, Encryption, Security, Data breach, Algorithms.*

1. Introduction

Cloud computing is one of the major fields in computer science. Cloud computing is making the life of people easy, whether it may be a developer trying to deploy an application over the internet or a stock trader who wants to analyse any company's stock-related data. Cloud can provide you with more than all the services you need. All you need is to log in to their console.

Cloud computing can be defined as renting services over any network. Cloud provides services varying from on-premises cloud setup to storing photos on the cloud for backup. These services can be majorly categorised into three types services - Infrastructure as a service, Platform as a service, and Software as a service, as depicted in Figure 1.

Along with these services, cloud computing provides cloud consumers with data storage-related services. Cloud consumers can store and operate their data on the cloud with a cloud provider that operates storage as a service. Cloud consumers can scale up or scale down their storage resources according to their business needs.

Cloud manages the storage and security of the data, and consumers can access the data over the internet or any network. Cloud consumers can get resources on a pay-as-you-go model that helps them save a lot of resources and money.

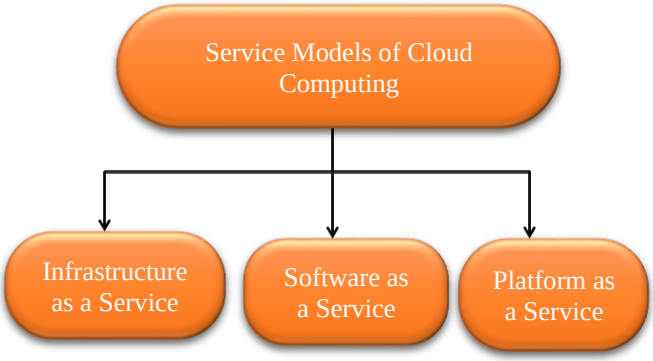

Fig. 1 Cloud Service Models

Also, consumers can manage their resources with the help of the cloud storage lifecycle. Cloud storage has been divided into the following three types: object, file and block storage.

2. Literature Survey

Achieving cloud storage security with flexibility requires combining various encryption algorithms [19]. This paper combined identity-based and attribute-based access policies for encryption techniques on cloud storage and analyzed the feasibility of the algorithms. The proposed system had security for cloud storage less secure than attribute-based access control. The authors briefly discussed

the security issues in cloud storage. They proposed work that shows encryption using the AES algorithm [11] using file encryption. The drawback is that the proposed system only works in stable internet connection and can only encrypt text files, not audio and video files.

AES algorithm's protection against Brute Force Algorithm is unbeatable because of encryption key size. This paper elaborates on a study to find that encryption time is highest (7.3 sec) for RSA and lowest (1.6 sec) for AES encryption algorithm, and medium (3.0 sec) for DES encryption algorithm. It is also observed that decryption of the AES algorithm runs in the least time (1.0 sec), and the RSA encryption algorithm takes the most time (4.9 sec) [15].

AES encryption algorithm [20] provided confidentiality and increased data security for cloud storage. The proposed application was hosted on an online cloud database provided by a US-based cloud service provider that stores its data online at different locations in encrypted form. Using a unique file ID and storing data at different locations decreased the chances of data breaches and made it more confidential. With different encryption algorithms, the file size of encrypted files increased drastically. As discussed in this paper, its implementation showed satisfactory results as Verilog code was used for AES encryption, which could be helpful in wireless communication in the military or wherever communication is less feasible [10]. Encryption was covered by key expansion, mix columns, add round keys, shift rows, and sub bytes transformation. Decryption was done using key expansion, inverse shift rows, inverse sub bytes, inverse mix columns, and inverse adds round key transformations. Still, it showed a disadvantage of every block being encrypted similarly.

The AES encryption algorithm faces a major drawback in securing data on the cloud. This paper studied the performance of the AES encryption algorithm [23] under different parameters. NIST nominated the AES encryption algorithm because it provided high computational efficiency and could be used at high speed in broadband links. The study used AES key expansion, add round key, mix columns, substitute bytes and shift rows transformation.

The widely used different encryption techniques as classified in Table 1.

3. Methodology and Implementation

The methods discussed till now tell us that the cloud is safe. When a consumer lends a service, he needs to think about two things: the safety of the cloud and the security in the cloud. The safety of the cloud is in good hands, but the safety of cloud is still questionable. The stats we have discussed clearly show that most attacks happen due to insecurities in the cloud. In this project, we have tried to improve security in the cloud using Fernet and KMS (key management system).

Table 1. Comparison of different encryption techniques

Factors	AES	DES	RSA	Blowfish
Size of Key	128,192,256 bits	56 bits	>1024 bits	32-448 bits
Memory Used (KB)	14.7	18.2	31.5	9.38
Size of Block	128 bits	64 bits	Min 512 bits	64 bits
Structure	Substitution permutation network	Balanced Feistel network	-	Feistel network
Algorithm	Symmetric	Symmetric	Asymmetric	Symmetric
Average entropy per byte of encryption	3.84	2.94	3.0958	3.39
Tunability	No	No	Yes	No
Security	Highest	Poor	Very High	High
Consumption of Power	Less	Less	Highest	High

3.1. Architecture Diagram

In this section, we will study different modules and their communication. We will look at the application's architecture and learn more about its functioning. In this project, we will create around six modules, each of which will have its separate purpose in the application. Refer Architecture diagram (Figure 3) to understand the flow of modules and the communication between them.

3.1.1. Front-end Module

This module will be built on Angular 10. It will be a single-page web application. That will be responsive to any screen size and provide users with a graphical user interface (GUI). It will be a console from which they can utilize the system's functionality. It will communicate to the Https module (server) and perform all the communication between the user and the server.

3.1.2. Firebase

It is one of the services from the google cloud computing platform. It is a database as a service. It will help us from authenticating a user to managing all the related key management systems. This module will be merged with the Https module and help establish the communication between the database and all other modules.

3.1.3. Https Module

This module is like the heart of the program and communicates almost with all other modules. This module will be built using express and node JS. Express Js will be used to establish the server and communicate with databases and APIs, whereas Node JS will help us code and perform the logical operations.

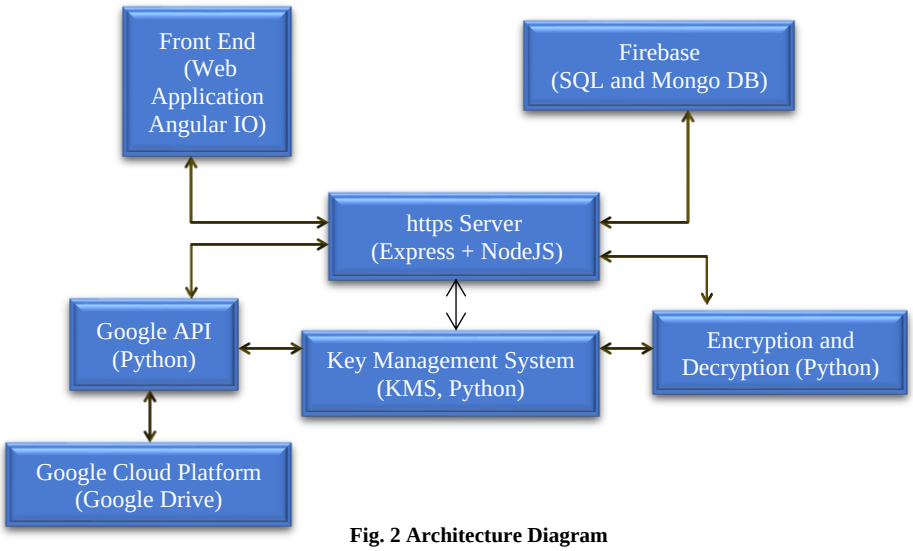

Fig. 2 Architecture Diagram

3.1.4. Encryption & Decryption

This module will be built upon python and handle everything related to encryption and decryption. It will also be responsible for generating keys and rotating them from time to time. This module will mostly communicate with the key management system module.

3.1.5. Key Management System Module

It is one of the most important modules as it will handle the Key Management system for the organizations or users. It will be coded in python and communicated to Https modules to make updates in the firebase, Google API module for file verification and other purposes, and encryption and decryption modules for Key related purposes. After the https module, this will be the next most active module in our application.

3.1.6. Google API Module

This module will be the one to manage google drive for the user. This module will canary out all the tasks like Upload, Download, search, authentication, etc. this module will be coded in python. And will communicate mostly to the https module or key management system module.

3.1.7. Google Drive (Google Cloud Computing Platform)

It is a cloud service provided by google cloud computing platform (GCP). It is stored as a service and will provide almost all storage-related services. It will be communicated to the Google API module.

4. Applications

The proposed application can be useful for the organization looking to improve the way of working in the cloud for safety scenarios. Our application can also be utilized by any individual who needs to store some sensitive

data over the cloud. In this project, we have tried to provide an application that will add an additional layer of security in the cloud.

Some of its applications also include user applications in an organization where data needs to be secured centrally in a secure environment for storing sensitive data.

5. Conclusion

This paper has researched different encryption techniques and key management systems. We came across various encryption techniques and learned a lot about them. We concluded to use a fernet algorithm. Fernet is a symmetric key encryption algorithm. Fernet utilizes two algorithms: Advanced encryption standard (AES) 128 in CBC mode for encryption and SHA256 HMAC for message code authentication. We will also try to implement a new key management system. The KMS we are currently working on will support additional features like spit keys and key rotation to make the application more secure.

With this project, the client can get a single-page responsive web application that any organisation or individual can utilize to improve security in the cloud and within the organization. This application is built on the latest technologies like Angular 10, NodeJS, ExpressJS, Typescript and Python.

As this application is built with new technology, new features can be implemented and solve testing time bugs easily, which gives this application a lot of future scope for research and development.

Acknowledgments

We want to thank the management for providing the essential resources required for the work.

References

[1] W. Fumy, and P. Landrock, “Principles of Key Management,” *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 785-793, 1993.

[2] D. Mazieres, M. Kaminsky, M. F. Kaashoek, and E. Witchel, “Separating Key Management from File System Security,” *in Proceedings of the Seventeenth Acm Symposium on Operating Systems Principles*, pp. 124-139, 1999.

[3] C. K. Wong, and S. S. Lam, “Keystone: A Group Key Management Service,” *In the International Conference on Telecommunications*, ICT, 2000.

[4] Arun Pratap Singh, Himanshu Pundir, "Secure File Storage on Cloud Using Cryptography," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 5, pp. 12-15, 2020. Crossref, https://doi.org/10.14445/23488387/IJCSE-V7I5P104.

[5] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, “Combinatorial Optimization of Group Key Management,” *Journal of Network and Systems Management*, vol. 12, no. 1, pp. 33-50, 2004.

[6] K. Lu, Y. Qian, M. Guizani, and H. H. Chen, “A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 2, pp. 639-647, 2008.

[7] Maryann Thomas, S. V. Athawale, "Study of Cloud Computing Security Methods: Cryptography," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 4, pp. 1-5, 2019. Crossref, https://doi.org/10.14445/23488387/IJCSE-V6I4P101.

[8] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A Distributed Key Management Framework with Cooperative Message Authentication in Vanets,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616-629.

[9] A. Ambekar, M. Hassan, and H. D. Schotten, “ Improving Channel Reciprocity for Effective Key Management Systems,” *In 2012 International Symposium on Signals, Systems, and Electronics* (ISSSE) pp. 1-4, 2012.

[10] M. Pitchaiah, and P. Daniel, “Implementation of Advanced Encryption Standard Algorithm,” 2012.

[11] D. Mukhopadhyay, G. Sonawane, P. S. Gupta, S. Bhavsar, and V. Mittal, “Enhanced Security for Cloud Storage Using File Encryption,” Arxiv Preprint Arxiv, 1303.7075, 2013.

[12] S. H. Seo, X. Ding, and E. Bertino, “Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructures,” *In 2013 IEEE International Conference on Smart Grid Communications* (Smart grid comm) , pp. 498-503, 2013.

[13] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo, “Wake: Key Management Scheme for Wide-Area Measurement Systems in Smart Grid,” *IEEE Communications Magazine*, vol. 51, no. 1, pp. 34-41, 2013.

[14] R. Arora, A. Parashar, and C. C. I, “Transforming, Secure User Data in Cloud Computing Using Encryption Algorithms,” *International Journal of Engineering Research and Applications*, vol. 3, no. 4, pp. 1922-1926, 2013.

[15] P. Mahajan, and A. Sachdeva, “A Study of Encryption Algorithms AES, Des and RSA for Security,” *Global Journal of Computer Science and Technology* , 2013.

[16] R. Chandramouli, M. Iorga, and S. Chokhani, “Cryptographic Key Management Issues and Challenges in Cloud Services,” *In Secure Cloud Computing* , Springer, New York, NY, pp. 1-30, 2014.

[17] N. Aleisa, “A Comparison of the 3des and AES Encryption Standards,” *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 241-246, 2015.

[18] N. Surv, B. Wanve, R. Kamble, S. Patil, and J. Katti, “Framework for Client-Side AES Encryption Technique in Cloud Computing,” *In 2015 IEEE International Advance Computing Conference (IACC)* , pp. 525-528, 2015.

[19] A. Nandgaonkar, and P. Kulkarni, “Encryption Algorithm for Cloud Computing,” 2016.

[20] M. P. Babitha, and K. R. Babu, "Secure Cloud Storage Using AES Encryption," *In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)* pp. 859-864, 2016.
[21] N. Islam, and M. K. V. Riyas, "Analysis of Various Encryption Algorithms in Cloud Computing," *International Journal of Computer Science and Mobile Computing*, vol. 6, no. 7, pp. 90-97, 2017.
[22] S. Thota, R. P. R. Induri, and R. Kune, "Split Key Management Framework for Openstack Swift Object Storage Cloud," CSI Transactions on ICT, vol. 5, no. 4, pp. 397-406, 2017.
[23] A. Abdullah., "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," *Cryptography And Network Security*, vol. 16, pp. 1-11, 2017.
[24] E. G. Ismail, A. Chahboun, and N. Raissouni, "Fernet Symmetric Encryption Method to Gather MQTT E2e Secure Communications for Iot Devices," 2020.
[25] S. S. Tyagi., "Enhancing Security of Cloud Data Through Encryption With AES and FERNET Algorithm Through Convolutional-Neural-Networks (CNN)," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, pp. 288-299, 2021.
[26] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52-64, 2003.
[27] W. Zeng, Y. Zhao, K. Ou, and W. Song, "Research on Cloud Storage Architecture and Key Technologies," *in Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human* , pp. 1044-1048, 2009.