Employability of Advanced Encryption Standard (AES) in enhancing the Safety Safeguards of Cloud Computing Data

Dhruv Khera

Pathways School, Noida

ABSTRACT

The number of people who use the internet is always growing. Every day, a lot of digital data is exchanged. Unauthorized access to some information is essential and must be prevented. Inorder to prevent unauthorized access to the original data, encryption techniques are essential. There are many different algorithms that can be used to encrypt data. The Advanced EncryptionThe standard encryption algorithm (AES), which is widely supported and utilized, is one of themost effective options. The purpose of this work is to show how to use cloud-based AES encryption and decryption to create secure file transfers. Files can be intercepted as they movefrom one location to another by hackers. Files can be easily hacked if they are not wrapped. Asa result, file transfer networks are safeguarded by the AES algorithm. It is said that if AES is used in file-sharing systems, thieves won't try to steal data when sending files. As per the review's discoveries, AES offers more insurance during information encryption and decoding during document moves without break from programmers endeavouring to deliberately take information.

INTRODUCTION

Computers are used for a wide range of activities these days, including gaming, designing, surfing the web, and transferring data or files. When transferring large amounts of data betweendifferent industries, having access to the internet is essential. However, transferring files acrossa network carries significant security risks. As a result, encryption employing the AES algorithm is a dependable strategy for safeguarding the file's contents during transfer and ensuring its safe arrival at its intended destination.

Because it provides the foundation of information, knowledge, and wisdom necessary to assistin making accurate decisions and achieving objectives, data is essential for any organization. As data grows exponentially, organizations need more resources to store and analyze it. Due toits numerous benefits, including scalability, dependability, and affordability, cloud computinghas emerged as a popular option. Cloud computing has many advantages, but it also has a lot of drawbacks, most of which have to do with security issues like data privacy and sharing concerns. Cloud servers are dependent on users' trust to store and manage their data, making them susceptible to misuse and unauthorized access. Additionally, data sharing among stakeholders may result in the disclosure of information to unauthorized third parties, either intentionally or unintentionally. Therefore, in order to guarantee the rapid expansion of cloud computing technology, it is essential to effectively address these issues. Among the many usesof the cloud are: 1) Hybrid Cloud; 2) Testing and Development; 3) Recovery; 4) Backup; 5) Applications for Image Editing; 6) Applications for Detecting Viruses; 7) Applications for Converting URLs; 8) Applications for Social Media; 9) Applications for Accounting; and 10)Applications for Management

AES REPOSITORY AND RETRIEVAL IN A CLOUD ENVIRONMENT

Several models for cloud-based data protection have been investigated and developed for numerous applications.

This article focuses on effective data protection by preventing leakage and identifying the 19 malicious entities that are responsible for leakage, as depicted. In most cases, data protection is achieved through leakage prevention and leak detection. Cryptography and access control mechanisms are used in the main ways to prevent data leaks.

The symmetric key encryption algorithm known as AES [7] is widely used to safeguard electronic data. In 2001, NIST decided to use it instead of the older Data Encryption Standard(DES) and Triple DES encryption methods. AES supports key sizes of 128, 192, or 256 bits and a fixed block size of 128 bits. Encryption and decryption are carried out by means of a structure known as a substitution-permutation network (SPN). As the de facto standard for encryption in a variety of applications, including electronic communication, onlinetransactions, and data storage, AES is regarded as extremely secure.

AES has proven to be a more secure and effective encryption algorithm, despite the fact that itis more difficult to implement than DES and Triple DES.

Its strength, dependability, adaptability, and ease of integration into existing systems are largelyresponsible for its widespread use.

How the cypher works: Instead of working with bits, AES works with data bytes. The cypher simultaneously processes 128 bits (or 16 bytes) of the input data because the block size is 128bits.

The following factors influence the number of rounds: round keys are made up of 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key. A Key Timetablecalculation computes all the round keys from the key. Therefore, the initial key is used to generate numerous round keys that will be utilized in the appropriate encryption round.

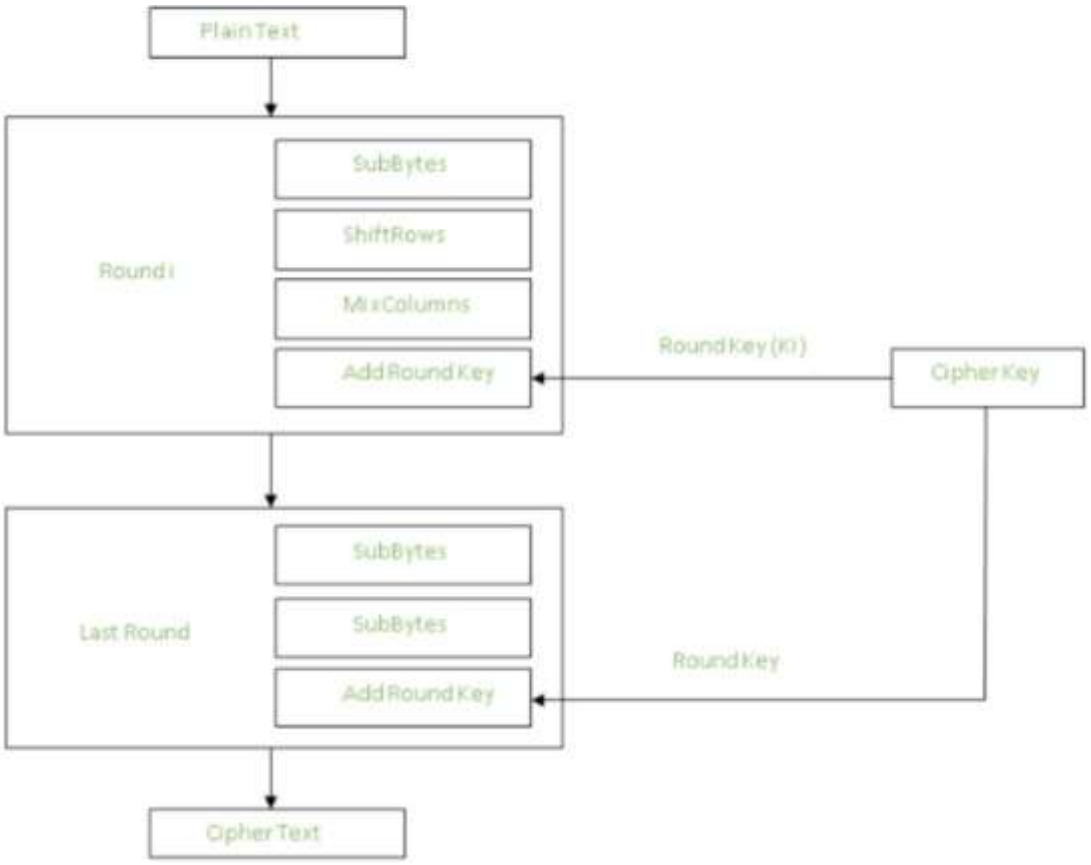

Figure 1: The Advanced Encryption Standard (AES) process

SYSTEM ARCHITECTURE

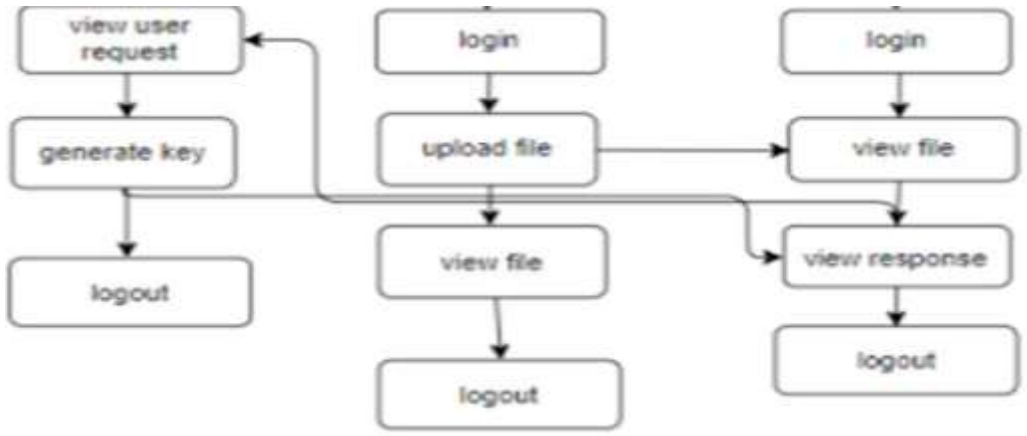

Figure 2: System Architecture

IMPLEMENTATION

The work process is broken up into modules.

1) The Data Owner requests access to TPA (Third Party Authority) via login.
2) Data User's request for TPA login.
3) The login credentials of both users and data owners are checked by Third Party Authority(TPA).
4) The Data Owner uploads documents.
5) File request from the user of the data
6) The user's request is approved by the administrator

A. Cloud Service Provider CSP will use the system's default login information to sign in.

1) Request a View: Csp examines a specific file's user request. The file key will be given to that user if he accepts.
2) Make a Key: The user will receive the key, which the Csp will generate.
3) Resign: At last, log out from the framework.

B. Owner of the Data

1) Registrations: The owner of the data will sign up using information like their name, email, password, confirm password, contact information, and address.
2) Login: When the CSP accepts the request, the data owner will log in to the system.
3) Submit Files: Files will be uploaded by their owner.
4) Look at Files: All files uploaded by the data owner will be displayed in cypher text to the owner.
5) Resign: Log out of the system at the end.

C. Users of the Data:

1) Registrations: The user of the data will sign up using their information, such as their name, email, password, confirm password, contact, and address.
2) Login: With the appropriate conditionals, the data user will sign in to the system.
3) Look at Files: All files uploaded by the data user will be displayed in cypher text format. The CSP will receive a request from the data user.
4) Read the Response: The request will be accepted by CSP, and the requested user will receive the key via email.
5) Resign: Log out of the system at the end.

D. Data Owner's Request for Cloud Service Provider (CSP) Login The data owner creates an account; The owner of the data must log in in order to access the homepage; The attempt to login will result in a request being sent to the Cloud Service Provider.

E. When requesting access to CSP, the data user also creates an account; The data user must log in if they want to go to their homepage first; The user's attempt to log in will result in a request being sent to the Cloud Service Provider.

F. The Cloud Service Provider (CSP) verifies login access for both users and data owners TheCloud Service Provider receives login requests from both users and data owners. The only thingCSP can do is validate their accounts. The OTP will then be sent to the registered email addressof that individual.

G. The Data Owner Can Upload Files The Data Owner Can Login After Entering the Key From The Mail The owner of the data will then upload the file or data. Additionally, it will be stored online.

H. Data User Request for Files Data users will also use the CSP's OTP key to log in. The information client will demand the information proprietor's record to an Administrator.

I. User's Request Received by Administrator will receive the user's request. The request can be accepted or rejected by admin. The member in question will receive the key if the administrator grants the request.

J. Data User Receives Key to Download Files After Administrator Accepts File Request The data user will receive the key. With the mystery key, information clients are currently ready to download the document or ready to securely see the document.

RESULTS

The screenshots of cloud computing using AES VIII are provided below the results. Conclusion: To guarantee the safety of digital data transfers, it is essential to employ encryptiontechnologies like the AES algorithm. Protecting important information from unauthorized access is essential in light of the rapid growth in internet use and the massive data exchange. One of the most effective encryption algorithms is the AES algorithm, which is widely used and endorsed. In general, encryption technologies like the AES algorithm are very important for keeping digital data transfers safe. To keep up with changing threats and ensure the safety of vital information, it is essential to continue developing robust solutions as technology advances.

Figure 3: Cloud computing Using AES

CONCLUSION

The use of encryption technologies such as the AES algorithm is crucial to ensure the securityof digital data transfers. With the rapid increase in internet usage and the exchange of massiveamounts of data, it is essential to protect vital information from unauthorized access. The AESalgorithm, which is widely endorsed and implemented, is considered one of the best encryptions algorithms in terms of efficiency. Overall, encryption technologies such as the AES algorithm play a critical role in ensuring the security of digital data transfers. As technology advances, it is crucial to continue developing robust solutions to keep up with evolving threatsand ensure the safety of vital information.

REFERENCES

1. Mohammad Ausaf Anwar, Durgaprasad Gangodkar, "Design and Implementation of Mobile Phones based Attendance Marking System", Department of Computer Science Engineering, Graphic Era University, Dehradun, Uttarakhand, India, 2015.
2. Jun Lio, "Attendance Management System using a Mobile Device and a Web Application", Department of Socio-informatics, Faculty of Letters Chuo University
3. Mahesh G, Jayahari KR, Kamal Bijlani, "A Smart Phone Integrated Smart Classroom", Amrita e-Learning Research Lab (AERL) Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham, Amrita University, India, 2016.
4. Ekta Chhatar, Heeral Chauhan, Shubham Gokhale, Sompurna Mukherjee, Prof. Nikhil Jha,"Survey on Student Attendance Management System", S.B. Jain Institute of Technology, Management and Research, Nagpur, 2016.
5. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).
6. Md. Milon Islam, Md. Kamrul Hasan, Md Masum Billah, Md. Manik Uddin, "Developmentof Smartphone-based Student Attendance System", Department of Computer Science and Engineering Khulna University of Engineering & Technology, Khulna-9203, Bangladesh, 2017.
7. Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.