2017 International Conference on Intelligent Computing and Control (I2C2)

Enhanced Cloud Data Security Using AES Algorithm

Akhil K.M
Department of Computer Science,
Amrita University, Mysuru, India.
(email: akhilkkvl@gmail.com)

Praveen Kumar M
Department of Computer Science,
Amrita University, Mysuru, India.
(email:praveenmrnambiar@gmail.com)

Pushpa B.R
Department of Computer Science,
Amrita University, Mysuru, India.
(email: preeths1@gmail.com)

***Abstract*— Cloud computing is the revolution through which individuals can share resources, services and data among the users through the network. Since millions of users uses the same network for data transfer, the data becomes more vulnerable to different security attacks from intruders. Providing security to these data has become the critical area of concern. The current system for data security concentrates on providing security to the stored data in cloud storage but concerns less on securing the data while it is being transferred. The data becomes prone to intruder attacks while being transferred. Also, in the current existing trend, the third party auditor is given access to data during data transfer. This also increases the access vulnerability of data as the intruder could act as third party and gain access to the data. Considering security as a crucial issue, the system proposed concentrates on providing security to transferring data using encryption technique. The system also takes into consideration the issue concerned with the third party auditor, that in the proposed approach, the auditor is denied access to the user data. Experiments are conducted and has shown that the proposed approach increases the overall security of system by making it difficult for intruders to crack the data being transferred.**

***Index Terms*— Cloud Computing, AES Data Encryption, Cloud Servers**

I. INTRODUCTION

Cloud computing is an anywhere anytime on demand service phenomenon which makes the cloud services available to its users irrespective of their geographical location. Cloud computing provides various services such as development environment, allocation and reallocation of resources, storage and virtual network capability etc. Cloud services could be pay per use or free services that are provided by various cloud providers such as amazon. Usage of cloud services has shown a drastic increase in recent years due to its wide service providing facilities and availability of services irrespective of its geographical locations.

Due to the high usage of the cloud services, imparting security to the user data has become more problematic in recent years. In this kind of wide networks, there are high chances of data loss or intruders penetrating into the network which increases data vulnerability. Providing security to data as well as secure access to users has emerged as main area of concern to the different cloud providers.

Providing secure data to the users includes providing security during data transfer and the data storage. The existing scheme for imparting security to data is concerned with data storage security and does not take into account of the intruding possibilities that could take place during data transfer. Also in the existing system, the third party auditor, is given access to view the user data which poses an increased threat to the user data as the intruder himself could mask as the third party. As the security is provided only for data storage, occurrences of data loss during transfer and intruders penetrating into the network increases.

A novel cloud data security model is proposed to overcome the different in-efficiencies in the current scheme of cloud security. In the proposed methodology, in addition to data storage security, it concentrates on providing security to transferring data using encryption technique and the approach makes the data un-available to the third party.

II. LITERATURE SURVEY

E.Thambiraja [1] discussed about some of the encryption algorithms which are currently in use. These algorithms mainly focuses on different encryption technics which are existing and comparison between the algorithms. Also discussed about the image encryption and information encryption. As a conclusion the survey explores that , all technics are useful in the realtime encryption but each technics has its own way. Which will be useful for different application.

Cong wang[2] concentrate on data storage security in cloud, which is an important feature of quality of service. To guarantee the correctness of user data in the cloud, an effective and bendable scheme with two relevant features is proposed differing to its prototypes. By applying the similar token with distributed authentication of cancelled data, the system accomplishes the combination of storage correctness insurance and data error localization, i.e., the identification of misbehaving server. The system is to guarantee the correctness of user data in cloud data storage, with explicit dynamic data support, with update, delete, and append.

Diaa Salama Abd Elminaam et.al [3] conducted a survey on various encryption algorithms like AES, DES, RC2, RC6, 3DES, Blowfish etc. 3DES algorithm is found to be less efficient compared to other algorithms regarding the throughput. Blowfish algorithm has better performance with respect to the changing packet size. RC2 algorithm consumes more power than the other algorithms. As a future work, these drawbacks of the existing algorithms can be considered and improved for better performance.

Anupama Mishra [4] discussed on various methods that enhances the security factors of transposition cipher. The proposed work insisted to add on strength to the classical

encryption method, transposition. This is achieved using ciphers in multiple level row transposition. Encryption ad decryption is done in two different levels with same and different keys. The double encrypted text is secured from a Brute force attack thus enhancing the simple cipher technique. The combination of two encryption methods namely cipher and transposition adds to the security.

Rupinder Kaur et.al [5] proposed a technique to choose among various encryption and decryption algorithms based on the user input file. Various symmetric key block algorithms like AES, RIJNDAEL, DES, 3DES, RC2 etc are discussed. Various input files like PDF, PPT, audio files, image files with varying sizes are considered. With respect to both encryption and decryption processes, RIJNDAEL algorithm gives better performance than the other algorithms for all types of input files. As a future work, a method to optimize the energy consumption of the security protocols can be considered.

Srinivasarao D et.al [6] discussed on various encryption algorithms like DES, 3DES, RC2, Blowfish, AES and RC6. Various parameters like encryption key size, encryption decryption time, CPU process time, power consumption, number of rounds etc are considered for a comparative study. The results show that the Blowfish methodology has the best secure unbreakable code and best throughput. 3DES has the least performance.

J. R. Ullmann [7] proposed a new algorithm for subgraph isomorphism. Brute-force tree-search enumeration procedure determines subgraph isomorphism. In the proposed algorithm, succeccor nodes in each tree search is eliminated to enhance the efficiency. Clique detection, directed graph isomorphism, graph isomorphism etc are randomly done to analyze the time consumed. Among these, the clique detection method is found less efficient. The major advantage of the algorithm is that it can well cope up with the undirected subgraph isomorphism.

Ali Mir Arif Mir Asif et.al [8] conducted a review on various classical and modern encryption techniques. Data privacy, confidentiality, integrity, authentication, authorization, validation, access control, timestamping, non-repudiation, revocation are some of the major security issues in cloud. Encryption algorithms like Caesar cipher, Vigenere cipher and Playfair cipher, DES and S-DES are discussed and compared based on avalanche effect. The comparative study reveals that Caesar cipher is the worst technique with respect to the avalanche effect.

Hari Krishnan Soni et.al [9] proposed a mixed encryption algorithm which is highly suitable for coding advanced language tools. The proposed algorithm is based on matrix calculation and bit shifting, making use of less computational resources. The proposed encryption algorithm involves symmetric cryptography where same key is used for encryption and decryption. The algorithm is compared with various existing algorithms like AES, DES etc and is found efficient. Least encryption time is the major advantage of the algorithm. As a future work, the security issue concerning the private key exchange can be considered.

V. Umakanta Sastry et.al [10] proposed a modified Hill cipher method in which the plaintext is interweaved with each iteration and multiplied with the key matrix. The repeated interweaving, along with cryptanalysis and avalanche effect makes the ciphering technique efficient that hardly any attacks can be performed on it. The overall idea is to develop a strong cipher with comparable encryption and decryption time. As a future work, the analysis can be enhanced in handling the cases of extremely large plaintexts.

Maged Hamada Ibrahim [11] proposed a method that resist a coercer attack namely, sender deniable public key encryption. In this scheme, the sender lies to the coercer and opens up a random message. Meanwhile, the receiver can later decrypt the original message and thus is secured from the coercer attack. The algorithm highly relies upon correctness, security and deniability. The sender proceeds both honest and dishonest encryption, for the receiver and coercer respectively. The major pitfall of the method lies in the assumption. The scheme assumes that the coercer approaches after the data transmission. The desired deniability fails when the coercer approaches before the data transmission. As a future scope, the scheme can be made efficient regarding the sender's local randomness. It can also be transformed to receiver-deniable scheme.

Sahdi R Masadeh et.al[12] proposed a wireless technique to enhance cloud security. The proposed secure WiFi (sWiFi) algorithm is based on HMAC cryptography algorithm and is compared with other existing algorithms like AES, DES, 3DES etc based on various parameters like data block size, platforms, efficiency of encryption and decryption mechanisms etc. The architecture is designed using automata theory. Data integrity is secured using a Message Authentication Code (MAC). The algorithm is built on 64 bit encryption and decryption. As a future work, the algorithm can be expanded to 128 or 512 bits.

Sudhansu Ranjan Lenka et.al [13] proposed an algorithm by implementing two algorithms namely, RSA and MD5 hashing. A combination of algorithms gives an advanced security to the data. The proposed algorithm provides a three-fold security like data security, authentication and verification. RSA algorithm ensures data confidentiality and MD5 ensures authentication. Providing digital signature and prevention from unauthorized access are taken care by MD5 hashing technique. All the user requests are encrypted using RSA algorithm. Only the authorized user with the private key has the privilege to decrypt the data and access it. In the database table containing the public and private key information, the user details are updated after hashing it using the MD5 hashing technique. The digital signature is authenticated by the algorithm for authentication purpose. Once it is done, the encrypted file is given to the user that can be decrypted using the private key. The major advantage is that, since the algorithms are run in different servers, the efficiency is improved and the chances of unauthorized access is reduced

Sudha Singaraju [14] discussed on the cloud security and proposed a method to ensure the same using RSA algorithm. Major issues of the cloud include privacy, confidentiality, data integrity, location, relocation, availability, storage, backup and recovery. In this work, RSA algorithm is used to encrypt the data to ensure security. Public and private keys are generated. Public key is known to all whereas private key is only known to the owner of the data. The advantage is that only the authorized user with the private key can decrypt the message thus enhancing the data security.

Akanksha Tomar [15] discussed on data security in cloud using Elliptical curve cryptography algorithm. The advantages of ECC are highly secure, data integrity and authentication, data confidentiality. The ECC algorithms also known as public key encryption. which can be used to create tiny, speedy and efficient cryptographic key. It provides protection mainly in three ways such as authentication, key generation and encryption. The system creates cloud and data security, by using digital signatures and encryption with ECC. After the comparison with RSA algorithm and ECC cipher text, ECC provides more level of security using less key size.

Akash kanthale [16] discussed a survey about performance of some of the cloud security algorithms. Author talks about different types of cloud , ie private, hybrid, and community cloud, where author select some research works which are related to encryption and cloud security. The comparison of such work shows that, AES algorithm is more efficient than RSA algorithms.

III. PROBLEM DEFINITION

The drawback of existing system is that it exposes user data to a third party auditor and is concerned only with security of stored data. The proposed system concentrates on providing secure data transfer in addition to denial of data access to the third party. For providing security during data transfer, Advanced Encryption Standard (AES) is used. The advantage of AES over other encryption techniques is that it supports encryption for huge amount of data and consumes only less time for its execution. As there are chances for users to transfer data varying from few bits to different large sizes, an encryption technique compatible to all data is selected. Encryption and decryption of the data is done at the user side while being sent for storage and retrieved from the server. The issue that has arises due to providing third party auditor the access to user data is met by denying the data access to the third party and its role is constrained to checking the authenticity of users at the time when user send request for data storage. As encryption and decryption happens at the user side, the chances of viewing the data by third party is ruled out.

IV. PROPOSED SYSTEM

The proposed system cloud server securing approach about securing the data send by the user, to the cloud servers. As the data is send for storage to the cloud servers, the data will be encrypted using AES encryption technique. The user verification for authenticity is done by the third party auditor, whose role also extends in selecting the server for storing user data. The role of third party auditor ends in a particular transaction once when the user is verified and the available servers are listed to the user. The third party auditor is unaware of the encryption and decryption process that takes place in the system. The illustration of the proposed cloud security model is depicted in Fig1.

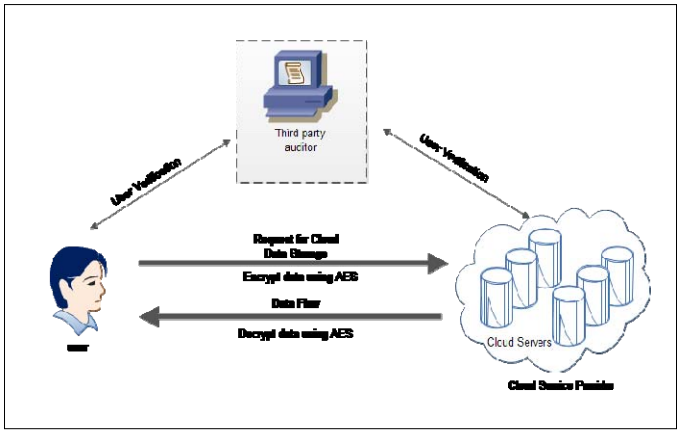

Fig1. Architecture diagram

The proposed security cloud server model works as follows :

- The user initiates the request for servers for data storage.
- As the server receives the request from user, it communicates with the third party for user verification.
- The third party sends the verification message to the user. Once the user is verified to be authentic, the users are provided with the servers that is available and could be used for storage.
- As the user gets the list of available servers, data is transferred to the servers.
- AES encryption takes place at the user side as and when the data enters the network. This reduces the possibility of intruders penetrating into the network and corrupting the data.
- The encrypted data is stored in the servers.

When the user request for data, the data is transferred to the user and the decryption occurs at the user side.

A. AES ALGORITHM (Advance Encryption Standard)

The acronym of AES is Advanced Encryption Standard, is a symmetric encryption algorithm which is designed to be effectual in both hardware and software. AES algorithm supports a block length of 128 bits and key size of 128,192 and 256 bits. AES performs all its operations in terms of bytes instead of bits, so AES treats the 128 bit as 16byte. This 16 byte is arranged in a 4X4 matrix.

AES is variable and depended to the length of the key. AES uses 10 series for 128-bit keys, 12 series for 192-bit keys and 14 series for 256-bit keys. Each of these series uses a different 128-bit series key, which is intended from the original AES key.

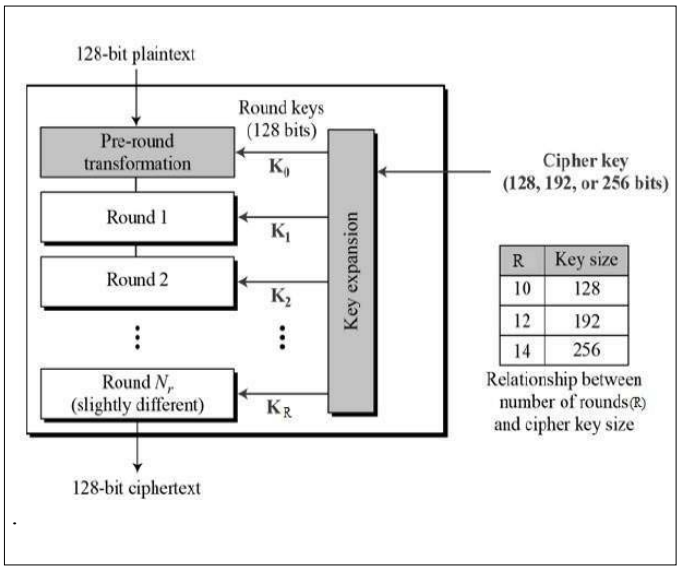

Fig2. Structure of AES

B. CLOUD SERVERS

Cloud is a large group of interconnected computers, any authorised persons or user can access these cloud services from any machines over the internet irrespective of the geographical location.

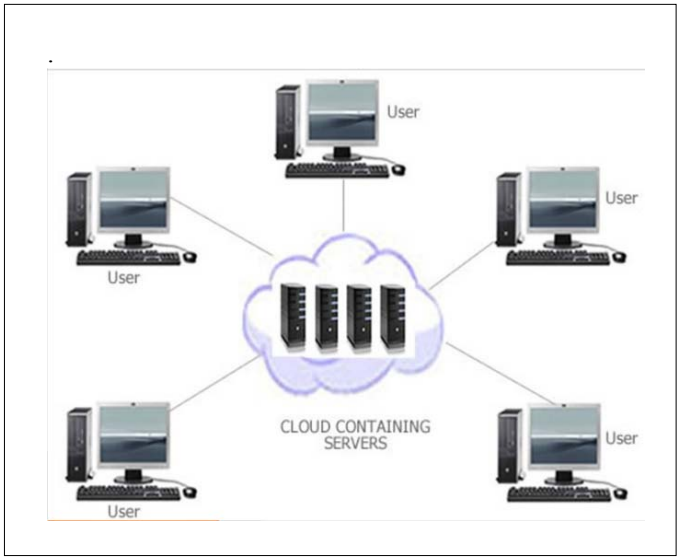

Fig3. Cloud architecture diagram

Cloud server is a logical server that is constructed, hosted and distributed through a cloud computing platform over the web. They retain and reveal similar capabilities and functionality and can be accessed remotely from any cloud service provider. In the proposed system the available servers are shown to the user, if the user is an authenticated user. And the list of files that particular user added into the same server also shown. The user can delete, update and download the already existing files with decryption from the server.

V. EXPERIMENTAL RESULT

The proposed system that is implemented in java platform, where the user can upload their files to the cloud using the upload portal. The registration of individual users are to be done in the portal initially for successful uploading and data storage in these servers.

The user provided data are encrypted by AES technique to reduce intrusion by third party intruders. Since the third party auditor does not have any role once the user is authenticated, it reduced the possibility of intruders masking the third party auditor for intrusion. The users will be restricted and the servers will be denied if the user does not prove to be authentic. The working model of the system is depicted as follows:

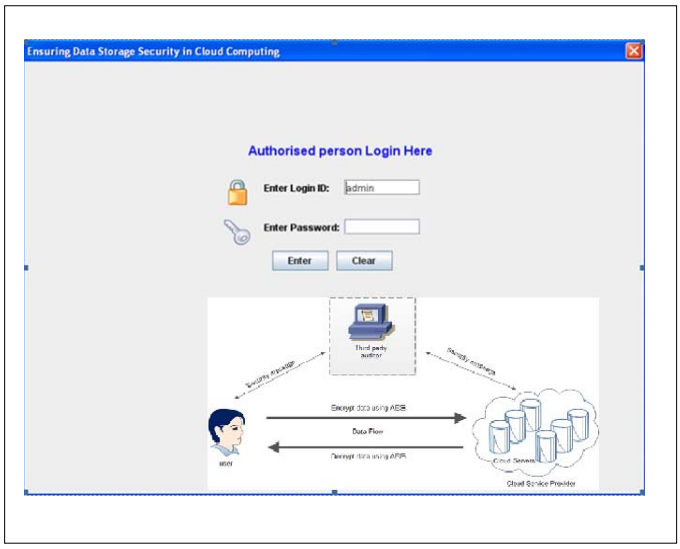

Fig4. Authorised person Login

Fig4, depicts the login for authorized users. Once the user is proved to be authorised, the server list will be forwarded by the third party auditor. If not proved to be authentic, the access to servers will be denied. Once the user is verified, the flow is depicted in Fig 5.

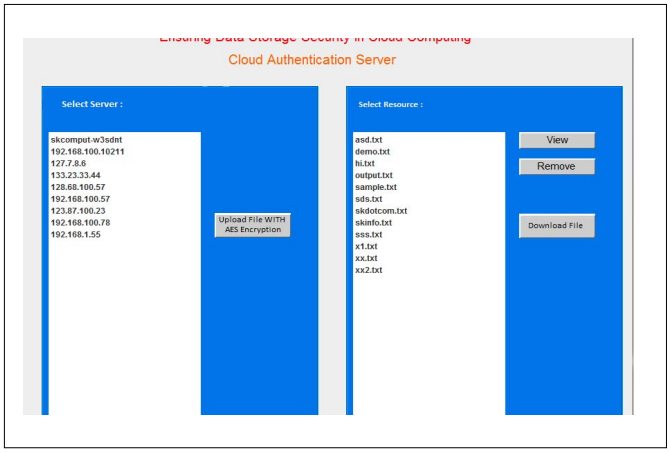

Fig5. Encryption and management

The above fig 5, gives the detailed view once when user is found to be authentic. List of available servers are provided to the user and user is given privilege to select the server for storage and the data is uploaded with AES encryption technique. User will be given access only to individual user files in the portal. The user could view, remove or download the existing user files and is denied access to all other files. This environment ensures secrecy of data to all other users who uses the same server for data storage.

VI. CONCLUSION

From the proposed AES based secure model for cloud data security, it has been clearly understood that proposed approach provides increased security to data while being stored and transferred. As AES encryption technique is used for data transfer, it rules out the possibility of the system to be un-available at times during the arrival of huge data. Since denial of access to the third party is done, possibility of intruders to mask as the third party and intrude into the network is avoided. Thus the proposed approach provides en efficient AES based encryption technique to cloud user data.

REFERENCES

[1] E. Thambiraja, "A Survey on Various Most Common Encryption Techniques," vol. 2, no. 7, pp. 226–233, 2012.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," 2009.

[3] D. Salama, A. Elminaam, H. Mohamed, A. Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," vol. 10, no. 3, pp. 213–219, 2010.

[4] A. Mishra, "ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT," pp. 327–332, 2013.

[5] R. Kaur, "Effective Symmetric Key Block Ciphers Technique for Data Security : RIJNDAEL," vol. 3, no. 7, pp. 2005–2008, 2014.

[6] D. Srinivasarao, S. R. N, C. Panchamukesh, and S. Neelima, "Available Online at www.jgrcs.info ANALYZING THE SUPERLATIVE SYMMETRIC CRYPTOGRAPHIC ENCRYPTION ALGORITHM (ASCEA)," vol. 2, no. 7, pp. 101–105, 2011.

[7] J. R. Ullmann, "An Algorithm for Subgraph Isomorphism," vol. 23, no. I, pp. 31–42, 1976.

[8] A. Mir, A. Mir, and S. A. Hannan, "A Review on Classical and Modern Encryption Techniques," vol. 12, no. 4, pp. 199–203, 2014.

[9] H. K. Soni, "A New Method in Symmetric Encryption for block cipher module : A Bit Shifting Approach," pp. 40–44, 2011.

[10] V. U. Sastry, N. R. Shankar, and S. D. Bhavani, "A Modified Hill Cipher Involving Interweaving and Iteration," vol. 11, no. 1, pp. 11–16, 2010.

[11] M. H. Ibrahim, "A Method for Obtaining Deniable Public-Key Encryption," vol. 8, no. 1, pp. 1–9, 2009.

[12] S. R. Masadeh, S. Aljawarneh, and N. Turab, "A Comparison of Data Encryption Algorithms with the Proposed Algorithm : Wireless Security," pp. 2–6.

[13] S. R. Lenka and B. Nayak, "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm," vol. 2, no. 3, pp. 60–64, 2014.

[14] P. Kalpana, "Data Security in Cloud Computing using RSA Algorithm," vol. 1, no. 4, pp. 143–146, 2012.

[15] I. Journal *et al.*, "SURVEY ON CLOUD SECURITY BY DATA ENCRYPTION USING ELLIPTIC," vol. 5, no. 12, pp. 992–997, 2016.

[16] A. Kanthale and S. P. Potdar, "Survey on Cloud Computing Security Algorithms," vol. 5, no. 4, pp. 2015–2017, 2016.

[17] ManiShankar, Sandhya R, and Bhagyashree S, "Dynamic load balancing for cloud partition in public cloud model using VISTA scheduler algorithm", Journal of Theoretical and Applied Information Technology, vol. 87, pp. 285-290, 2016.

[18] S. Gokuldcv and Radhakrishnan, R., "An improved log-based scheduling and load balancing in computational grid", International Journal of Applied Engineering Research, vol. 10, pp. 33819-33825, 2015.