IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 2, February 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Improved Advanced Encryption Using Four Square Cipher for User Anonymity and Untraceability in Mobile Cloud Computing

Solomon Babatunde Olaleye[1] and Shrikant Ojha[2]

[1]Research Scholar, Department of Computer Science & Engineering, Sharda University, Greater Noida, 201306, India
[2]Dean Research, Research and Technology Development Centre, Sharda University, Greater Noida, 201306, India

Abstract

One of the recent technologies is the integration of the mobility into cloud computing in order to form the mobile cloud computing (MCC). Data security and privacy have become critical concerns in distributing files to mobile users. An improved advanced encryption standard algorithm is designed in this paper to transmit users' files securely. The proposed algorithm uses extended version of the four square cipher to generate the secure key, which enhances the security for the users' anonymity and untraceability. This study enhances the number of rounds (Nr) in AES to 18. Though it consumes more time for encryption and decryption but make complexity for the attackers to hack user data. While comparing to the existing methods; data encryption standard and advanced encryption standard, the proposed improved AES enhances security of files better.

Keywords: *User Anonymity, Improved AES, Four Square Cipher, Multi-owners applications.*

1. Introduction

Nowadays, mobile devices are broadly utilized in majority of the advancing and advanced countries like USA and UK, the mobile phones penetration level have obtained 80 % in 2015 [1]. They are utilizing the smart mobile devices for flexible services like entertainment, work and knowledge sharing purpose. Need for computing power in the smartphone devices is still increasing because the mobile user's needs to run the certain important applications like as virus scanning, face detection and argumentation reality on the mobile phones [2]. The main objective of the smartphones is to provide easy intersection with users, which can perform as a PC when linked to a monitor, which has been developed recently. Though the mobile technologies have been improving steadily, but it would not satisfy certain requirements of the users [3]. It is featured with inherited characteristics of the mobility, which is termed as highlighted service for mobile cloud computing. Nevertheless, a resource suffers from computation, battery and storage that can interrupt the vision of location, system and time based ubiquitous computing system [4]. However, computational power and battery life still remains as the important concerns in the mobile devices. Mobile cloud computing (MCC) provides solution to these types of issues, especially by using offloading algorithm in the mobile work load to reduce the energy consumption. In this manner, energy reduction occurs even during application performance in smartphones [5-7].

In the previous works [8], the mobile cloud computing fields have been analyzed and examined in terms security aspects. In the [9], they demonstrated a substantial review of mobile cloud computing and its heterogeneity nature in the mobile devices. It also illustrated about the definition of mobile cloud computing and discovered the important elements required in the mobile cloud computing. An overview of MCC is represented with several challenges and illustrated in taxonomy diagram, see figure.1. The enlightenment features of MCC would encourage in detecting the future research directions.

Here, the various elements involved in the MCC are presented.

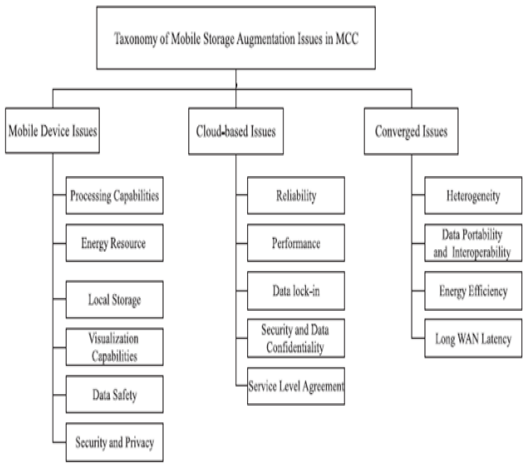

Fig. 1: Taxonomy Diagram of MCC [3]

Basically, MCC technologies have been developed from the surrounding environment like cloud computing, mobile internet and mobile devices. Therefore, by combining the benefits of the various technologies allow users to process data offloading and data storage at the remote servers. Apart from these benefits, there are also certain important issues that have to be taken care of. One of the significant problems is data security and privacy concern in MCC. Since, the mobile cloud computing is an open platform; it can be vulnerable to the attackers and hackers. Generally, the mobile cloud service providers (MCSPs) provide information security through virtualizations and firewalls. Nevertheless, these schemes would not prevent the user's privacy data from the mobile cloud service providers because of the untrusted remote cloud servers [7]. As to prevent the sensitive data against misbehaving adversaries, various security schemes like user credentials, session key generation and mutual authentications are considered for authentication mechanism. It is mainly designed for providing the secured data transmission from the data owner to the mobile cloud computing, see Figure 2.

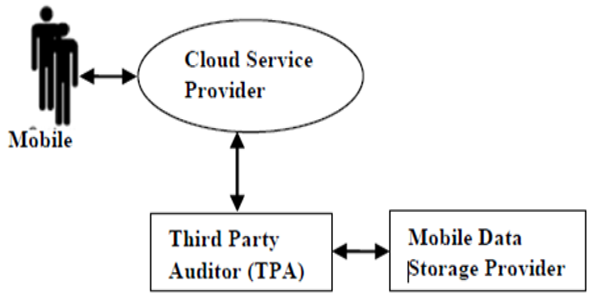

Fig.2: Secure Data Transmission in MCC

Prior encryption processes have certain drawbacks in terms of the security. Hence, security issues are classified into four domains; *Integrity*, *authentication*, *key generation* and *non-repudiation*. The key generation and verification for the secure communications in the existence of the third parties are referred as adversaries. It is associated with developing and examining the key authentication processes and deal with different aspects relevant to the data security [9].

The well-established method to prevent the sensitive private data from the attackers is to encrypt the data through cryptographic technique before transmitting the file to the mobile cloud. Then, it retrieves the data back through the secure key verification method over the encrypted data [10]. Though encryption technique provides the marginal security to the data files from the attackers, it is significantly inactive to consider the larger file sizes. Moreover, the authorized user needs to retrieve some files from the mobile cloud, which requires communicating with the mobile cloud service providers and permits the authorized user to perform over the secure encrypted data files [9]. To obtain significant data retrieval, it is suggested to receive the most related data files instead of receiving entire files. However, it is very toughest process to retrieve the data in secure and significant way in order to meet the requirement of multi-owner applications.

But in conventional method, public-key cryptography operates with 256-bit elliptic curve cryptosystem (ECC) to provide equivalent level of security as 3072-bit RSA public key which is in ratio 1 to 12 mathematically [11]. Thus, ECC is more efficient for mobile users while comparing with RSA method. In these traditional cryptosystems, a mobile user needs to spend additional computational cost to verify public keys of others. However, more storage space is needed to store public keys of others along with their corresponding certificates in the user's device. Hence, most of the existing methods like unidirectional authentication scheme, two party authentication scheme and SSO (Single-Sign-On) schemes are unsuitable to adopt in distributed mobile cloud environments [12].

In this paper, it analyzes data privacy and security issues in the mobile cloud computing. It proposes an improved advanced encryption standard algorithm in order to transmit the files securely for multi-owner applications. The proposed algorithm uses extended version of the four square cipher to generate the secure key generation, which enhances the security for the user anonymity and untraceability. The data owner file has to be protected from privacy violations; it encrypts the data before transmitting file to mobile cloud service through proposed improved AES algorithm. It further estimates the information security by comparing with existing AES algorithm, as the proposed system consumes higher time for encryption and decryption and makes complexity for the attackers to hack the data which improves the security. This paper is organized as follows: Section II represents the survey of various authors in improving the security of mobile cloud computing and moreover describes about the proposed concept, whereas III and IV demonstrate the experimental results and the conclusions.

2. Literature Review

Mobile cloud services have been establishing in recent years. Some authors concentrate on context extracted

system of mobile cloud computing [10]. On another side, some authors concentrate only on the demand of the users in cloud service communicating policy [11]. Moreover, certain quantity of works focus on the mobile cloud computing security, which describes about enhancing the security and the storage processing capacities that enabled the widespread adoption of MCC [10]. Researchers have investigated issues like energy consumption, resource utilization and security, providing brief description about application development and scalability.

Hence, some of the significant and secure techniques have been introduced to protect the secure communicating policy process in the mobile cloud computing environment. Furthermore, the need and demand of utilizing the data privacy preserving mechanisms are always proclaiming in the mobile cloud computing applications system. The encryption techniques have been broadly adopted in enhancing the security using cryptographic primitives, which concentrates on the security formalization, definitions and improving overall performances. The encryption method for the symmetric key was utilized to permit the data owner to outsource its own data, which is symmetrically ciphered towards the untrusted server. Song et al (2000) [13] proposed the notion of the symmetric encryption scheme for searching mechanism, that identified each word in the file encryption under a particular method of the two layer schemes of decryption. Hence, the time taken for searching process is linear in the file transmission. Then, Goh et al (2003) [14] proposed new method to minimize the workload on searching queries demand in the collected file systems. The proposed method is designed with bloom filter based file index mechanism, but it is directly proportional to the size of the file collection which in turn can increase the operating time. Later on, Chan and Mitzenmacher et al (2005) [15] depicted the secure encryption in the file searching scheme, which was slightly heavier than the previous methods. Even though the adversaries' models have not been taken into account, but it could produce the queries as per the result of the previous queries. However, they failed to improve the efficiency of the system.

In Li et al (2009) [16] a new ID-based encryption method for cloud computing environment was presented. Even though, author's new authentication would not accomplish untraceability and user anonymity. To overcome from the above mentioned issues, Liu et al (2012) [17] represented privacy preserving keyword searching mechanism for the cloud storage using the Elliptic Curve Cryptography (ECC) algorithm. It permitted the cloud service provider to do encryption process and resend the encrypted data with specific security keywords without knowing any data. However, this method did not help in the ranking based keyword search.

Yu et al (2013) [18] presented two round encryption scheme in order to avoid the data leakage. They provided users to enable on the server side with cipher text for double authentication. The main drawback of this system was the communication and computation cost which is quite higher. Furthermore, it performs on two round communication methods to recover the files from the server.

Recently, Tseng et al (2015) [19] introduced a list-free authentication mechanism for different server architecture system using bilinear pairings schemes. It has figured out the innovative and emerging issue to design a list-free Ephemeral Secret Leakage (ESL) method for resisting attacks. Therefore, SSO authentication methods have been utilized ID based encryption method for providing secure multi-server environment. However, author fails to contribute to the untraceability and user credential privacy method, as it forwards the user identity in plain text. Then Nitan Nagar et al (2016) [20] provided the new dimension for the MCC by proposing security algorithm for cloud storage. Their proposed scheme was against mitigation attack, which ensures the data is securely stored in the mobile cloud environment but the overall performance is significantly lesser.

3. Improved Advanced Search Encryption Via Four Square Cipher

In the proposed work, it aims to improve the data security and enhances resource management utilization in the mobile cloud computing. It proposes secure framework to provide security for data transmission in an efficient manner over multi–owner applications. In this paper, Advanced Encryption Standard algorithm (AES) was improved to ensure security and provide solution to untraceability and user anonymity in the MCC. The proposed work gives several merits over previous works.

The proposed secure framework provides solution to the untraceability and user anonymity using an improved AES algorithm. It provides the information security and data transmission in MCC with significant cryptographic method. It consists of important factors such as security checker, authentication verifier and location tracker and these are utilized to defend user anonymity very powerfully. Then, proposed mechanism defend the various attackers like service hijacking, malicious insider attack and logging attack to protect the mobile user data. It

proposes multi-way authentication method using improved AES algorithm that resolves the user anonymity, untraceability, non- reputation and overhead issues.

This research paper designs a secure architecture in the MCC, which consists of improved advanced search encryption via four square ciphers. It executes six important steps. They are: a) Authority Authentication b) Mobile cloud service provider c) Data Owner d) Mobile Users e) Improved Advanced Encryption Standard via four square cipher d) Authority Verification. These are explained as follows:

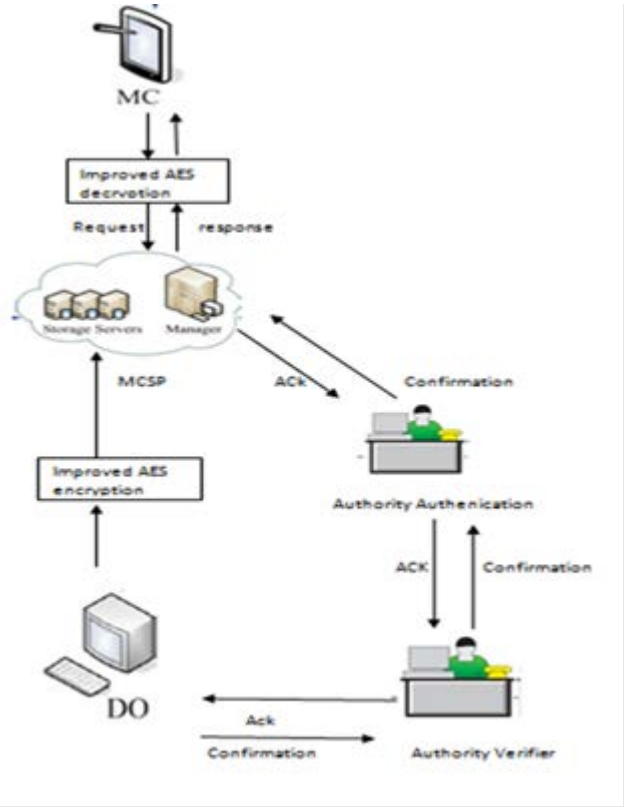

Fig.3: The Proposed Work Flow

As shown in Fig. 3, the design system architecture for user anonymous and data access control in mobile cloud computing consists of six entities such as:

A) Authority Authentication
B) Mobile Cloud Service Provider
C) Data Owner
D) Mobile Users
E) Improved AES Algorithm via Four Square Cipher

1. Generation of Key
2. Improved AES Encryption
3. Improved AES Decryption

F) Authority Verification

3.1 Authority Authentication (AA)

The authority authentication (AA) is an entity that generates public key parameters and secret key using four square ciphers. As a complete trusted authority in the control access method, it takes responsibility of providing confirmation and acknowledgement to the cloud service providers through authority verifier from the data owner.

3.2 Mobile Cloud Service Provider (MCSP)

Mobile cloud service provider (MCSP) comprises of the service manager with higher cloud storage servers. It takes charge of conserving encrypted data from the data owner and provides the guidance for accessing the outside users. MCSP has greater storage capacity and higher computation power.

3.3 Data Owner (DO)

In this step, the data owner is a user, who own files and desires to transmit the data files to another independent mobile cloud server. It is the main reason that determines anonymous to execute the access policy on its own data file before transmitting file, whereas cipher texts are stored in the MCSP using the improved AES algorithm for the authority verification purpose.

3.4 Mobile User (MU)

The mobile user is defined as resource reserved user, who determines the user anonymously access on the secured data hosted in the mobile cloud storage servers which is handled by the MCSP. When MU holds the set of key generation from improved AES algorithm, which is used for encrypting the plain text into cipher text with desired key size and significantly decrypt the encrypted data. Further, authority verification is performed to transmit the data from data owner to mobile users.

3.5 Improved Advanced Encryption Standard Cipher

The proposed improved advanced encryption standard functions like AES except that the number of rounds is increased. The conversion of plain text into cipher text according to the AES algorithm takes 10 rounds for a 128 bits key size, but this work increases up to 18 rounds by using four square cipher. The initial key generation takes place using polybius square for AES algorithm. It utilizes four square ciphers for key generation process. The AES

encryption steps are SubBytes, Shiftrows, Mix columns and Add round key which is described [21].

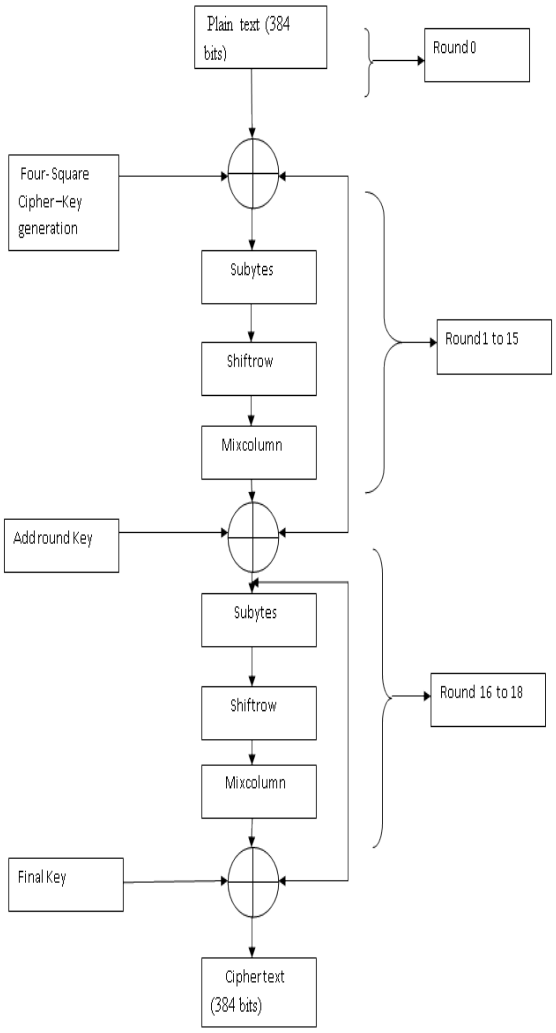

Fig. 4: Improved AES Encryption Algorithm

This work used 384 bits instead of using 128, 192 and 256 bits from AES algorithm. From this analysis, it has been identified that the AES elements execute based on its key size. In this proposed improved AES algorithm, the number of rounds has been increased to 18 rounds, whereas original AES has 10, 12 and 14 rounds for the 128, 192 and 256 key sizes respectively. The proposed system securities have been enhanced for user anonymity by adding the number of rounds higher than the existing AES algorithm. Figure 4 and figure 5 have clearly described the proposed system models, which highlight the number of increased rounds in order to provide higher security for the user anonymity and untraceability. It is considered that no modification in transformation would permit the breaking the AES algorithm. Hence, key sizes of 384 have been selected for resolving the security issues like user anonymity and untraceability.

This research extends the key size to 384 bit from 256 bit key size which in turn increases 14 rounds of AES to 18 rounds. In this mechanism, the secret key is generated using four square cipher [22], The improved AES algorithm is processed using for major steps; Subytes, ShiftRows, Mixcolumns and add round key for both encryption and decryption processes, which are explained below:

3.5.1 Subytes

It is referred to byte-by-byte substitution with 16x16 matrices, in which bytes are substituted individually with the help of S-box (Substitution table) [21]. It classifies each input by using 24-bit pattern, which can be interpreted using hexadecimal value. It comprises of 256 eight bytes through permutation value along with combination of GF (2^8) arithmetic operation and bit mapping. For instance, the hexadecimal (85) where 8 is taken to row and 5 is moved to column that results in s-box [21]. In the same manner, inverse Subytes transformation is carried out using inverse S- box for decrypting the cipher text into plain text.

3.5.2 Shiftrows

The main reason for this process is to give the diffusion of the bits over several rounds. The row 0 in the matrix is not moved, 1st row in the matrix is shifted by one byte, 2nd row is shifted by two bytes over left and 3th row is shifted by three bytes over left. Here, shifting of rows is continually performed to the left. Such type of transformation is usually carried on the matrix which comprises of columns and rows processing with higher security. The inverse shift rows is utilized by an improved AES decryption process, in which reverse to the shift row transformation as the rows are moved towards to the right side and the same process is followed in the steps as shown in figure 5.

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 2, February 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

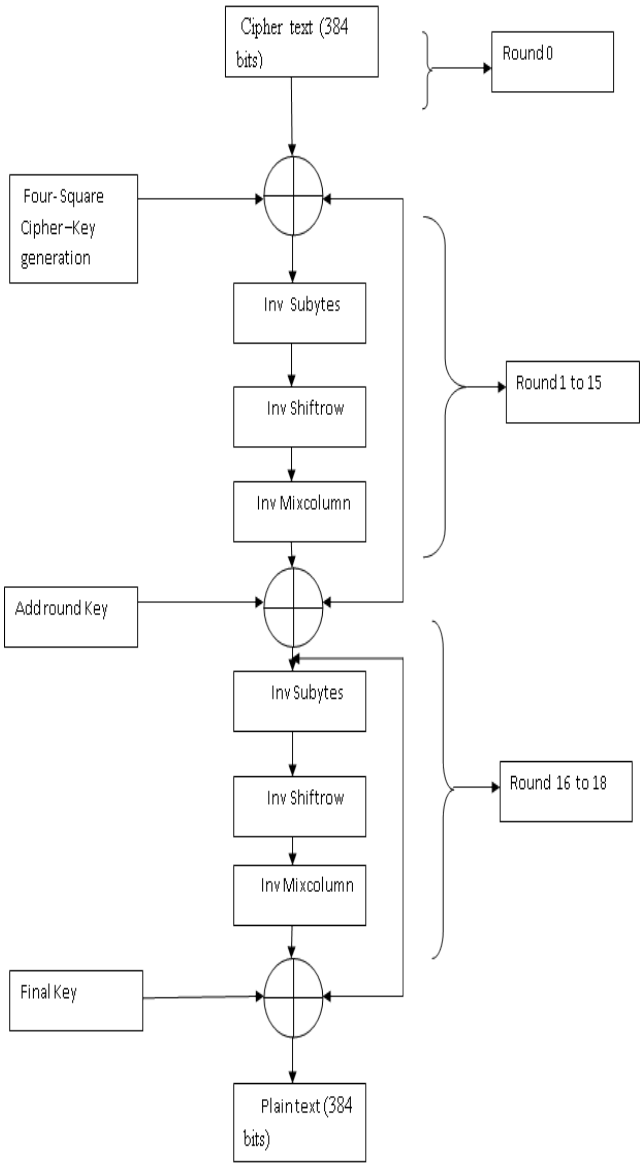

Fig.5: Improved AES Decryption algorithm

3.5.4 Mix Columns

The mix columns purpose is similar to the previous step, which aims to give the diffusion of the bits over several rounds. This is accomplished by multiplication operation of per column at a time. Then, each row is multiplied against every column in standard matrix. Therefore, the obtained values of this multiplication have undergone XOR operation together. For instance, First byte of B1' is multiplied with 01, 02, 03 and 03 and XORed to generate fresh B1" of the resulting matrix [21]. Hence, the multiplication maintains against one matrix row at a time against each value of a state column, which has formed the polynomial matrix. The inverse mix columns are utilized using an improved AES decryption process.

3.5.5 Add Round Key

In this process, round key is formed by using XOR operation with the matrix. The real key comprises of 128 bits, which is demonstrated in 4x4 matrixes. It is executed in column-wise in between the state column of the four bytes and the byte level operation is performed to get the round key per word. Therefore, inverse add round key executes XOR process in the cipher text and elaborate keys which are corresponding to the specific iteration. For example, if the picture on the left demonstrate the cipher and the key values, the last obtained value is produced based on the above process.

3.5.6 Key Generation Process via Four Square Cipher

This work uses enhanced version of the four square cipher technique, that consists of 10x10 matrices to produce the cipher text. The proposed improved AES algorithm permits the plain text including the numerical and alphabets (special case and capital letters). The users can very simply encrypt the combination of numbers, alphabets and characters significantly. It can accept almost 64 characters at the simple encryption [22], which provides secure data transmission. For an example, the plaintext "UNIVERSITY" when encrypted can become as "yN'X} _.N4Y" in cipher text as can be seen in figure 6.

Fig.6 Four Square Cipher

3.6 Authority Verification

After the successful completion of improved AES algorithm process, it allows user to access data which is approved by the authority verification. It provides acknowledgement and confirmation to the data owner and once after their approval, data can be accessed by the mobile users through mobile cloud service provider.

4. Performance Analysis

In this section, the performance analysis was performed Intel (R) Pentium (R) Core 2 Duo CPU 2.4 GHz (Virtualization Technology enables machine), 8 GB of RAM, and Ubuntu 14.04 (Long Term Support) runs on Linux. To improve the security of the mobile cloud computing, we used the JAVA language for the development of the proposed algorithms. The parameters that are considered for evaluating the performance of the improved algorithm in MCC are security, integrity, authentication and authorization in the data transmission. The proposed improved AES algorithm was compared with existing methods such as Data encryption standard, Advanced Encryption standard in respective to the computational time for the various file sizes. The results are recorded. The experimental results proved that computational encryption and decryption times can secure files very significantly than the existing approaches, see table 1.

Different file sizes from 20 Kb to 400 Kb have been taken as the input file sizes, computational encryption time and decryption time results for DES, AES and proposed improved AES algorithm are presented in table 1 and the charts plotted for clear comparison are shown in figure 7 and figure 8 respectively. Though the improved AES algorithm takes more time to encrypt and decrypt files due to increase in the number of encryption rounds and decryption rounds, yet it enhances the security of files in the data transmission to and fro cloud than existing algorithms.

Table 1: Encryption and decryption time for different file sizes

Input file size (KB)	DES		AES		Improved AES	
	Encryption (ms)	Decryption (ms)	Encryption (ms)	Decryption (ms)	Encryption (ms)	Decryption (ms)
15	20	24	35	39	46	49
78	63	70	81	87	95	108
198	133	146	147	141	161	163
224	142	144	154	155	169	172
386	151	147	169	161	182	180

4.1 Experimental Results

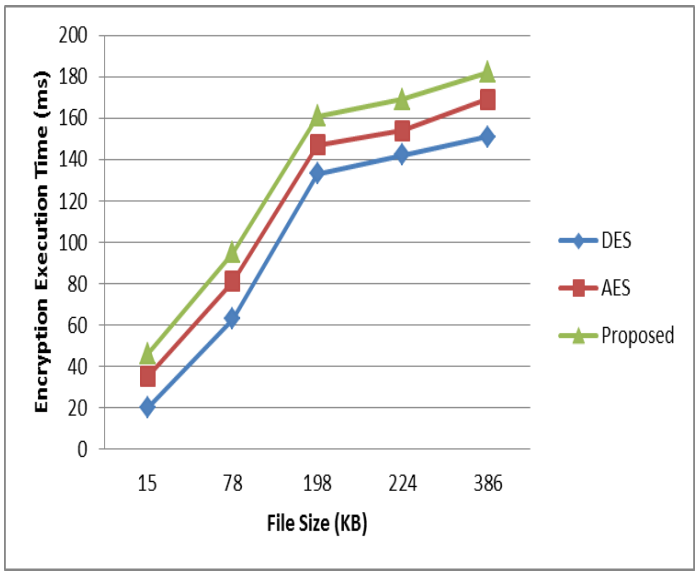

Fig. 7 Comparison of Results for Encryption

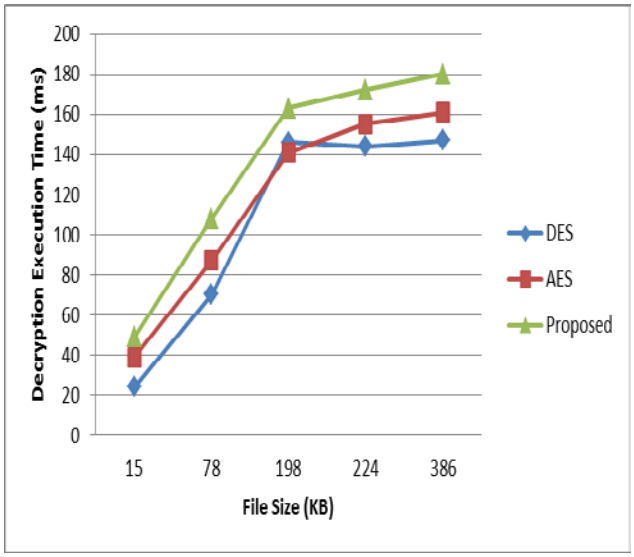

Fig. 8 Comparison of Results for Decryption

5. Conclusion

The developing field of mobile cloud computing suffers from security and data privacy issues due to the resource restrictions, unstable wireless environment and mobile devices. The data–intended mobile cloud services require higher security for user anonymity and untraceability of the mobile users. The files of the data owner have to be protected from privacy violations. In order to enhance the data security, at first data owner encrypts the data before transmitting to mobile cloud service through the authority verification using proposed improved AES algorithm. This improved algorithm enhances the security of user files and provides less chance for the attackers. Due to higher number of rounds than the existing AES algorithm, the proposed model consumes higher time for encryption and decryption and makes higher complexity for the attackers to hack the data as well. The key generation has been produced by the four square cipher that generates longest and toughest cipher text. Hence, while comparing with other methods such as AES and DES; it proves that the proposed algorithm obtains higher time for encrypting the data, which in turn enhance data security in the mobile cloud computing. In the future work, this work aims to study and provide secure resource optimization technique in the MCC.

References

[1] Billion Consumers Worldwide to Get Smart(phones) by 2016. /number-of-smartphone-users-worldwide/(last accessed 20 May 2016).

[2] 6.1B Smartphone Users Globally By 2020, Overtaking Basic Fixed Phone Subscriptions. 2020-overtaking-basic-fixed-phone-subscriptions/#.ok6rcs4:RPIH (last accessed 20 May 2016).

[3] K. Jongkil, S. Willy, Au Man Ho and S. Jennifer, “Adaptively Secure Identity-based Broadcast Encryption with a Constant-sized Ciphertext”, IEEE Trans. Inf. Forensics Security, 2014, pp.1–15.

[4] S. Abolfazli, Z. Sanaei, M. Alizadeh, A. Gani, F. Xia, “An Experimental Analysis on Cloud-based Mobile Augmentation in Mobile Cloud Computing”, IEEE Trans. Consumer Electron. 60 (1), 2014, pp.146–154.

[5] J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, “Provable Data Possession of Resource Constrained Mobile Devices in Cloud Computing”, Journal of Networks, 2011, pp. 1033–1040.

[6] J. Xu, E.C. Chang and J. Zhou, “Towards Efficient Provable Data Possession in Cloud Storage.” https://eprint.iacr.org/2011/574.pdf (last accessed 20 May 2016).

[7] P. Kumar, S. B. Rana, “Development of Modified Polybius Technique for Data Security”, Int. J. Innov. Eng. Technol, Vol. 5, 2015, pp.227–229.

[8] M. Shiraz and A. Gani, “A Lightweight Active Service Migration Framework for Computational Offloading in Mobile Cloud Computing”, J. Supercomput. Vol. 68, No. 2, 2014, pp. 978–995.

[9] T. Danova, “The Smartphone Report by Country: Adoption, Platform, and Vendor Trends in Major Mobile Markets Around World 2015, http://www.businessinsider.com/, accessed 10th January 2017

[10] P. Chaudhari, M. Das, and A. Mathuria, “On Anonymous Attribute Based Encryption”, in Proceedings of the Information Systems Security, in: LNCS 9478, 695 Springer, 2015, pp. 378–392.

[11] L. Cheng, Q. Wen, Z. Jin and H. Zhang, “Cryptanalysis and Improvement of a Certificateless Encryption Scheme in the Standard Model”, Springer Comput. Sci., 2014, pp. 163–173.

[12] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, W. Shi., “Ciphertext-policy Hierarchical Attribute-based Encryption with Short Ciphertexts”, Inf. 699 Sci., 2014, pp.370–384.

[13] D. Song, D. Wagner and A. Perrig, “Practical Techniques for Searches on Encrypted Data”, In

Proceedings of the IEEE Symposium on Security and Privacy, California, 2000, pp. 44–55.
[14] E. J. Goh, "Secure Indexes, Technical Report, Cryptology, ePrint Archive; 2003 http://eprint.iacr.org.
[15] Y. C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data", In Proceedings of Third International Conference on Applied Cryptography and Network Security. New York, 2005, pp.442–455.
[16] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based Authentication for Cloud Computing", In Proc. of Cloud Computing, Springer, 2009, pp.157–166.
[17] Y. Lu, "Privacy-preserving Logarithmic-time Search on Encrypted Data in Cloud", In Proceedings of 19th NDSS. San Diego, California, USA; 2012.
[18] J. Yu, P. Lu, Y. Zhu, G. Xue and M. Li, "Toward Secure Multi-key Word Top-k Retrieval over Encrypted Cloud Data", IEEE Trans Depend Secure Computing, Vol. 10, No. 4, 2013, pp. 239–250.
[19] Y. M. Tseng, S. S. Huang, T. T. Tsai, and J. H. Ke, "List-Free ID-Based Mutual Authentication and Key Agreement Protocol for Multi-server Architectures", IEEE Transactions on Emerging Topics in Computing, Vol. 4, No. 1, 2015, pp.102–112.
[20] N. Nagar and U. Suman, "A Secure Mobile Cloud Storage Environment using Encryption Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 140, No.8, 2016.
[21] A. Kakkar, M. L. Singh and P. K. Bansal, "Efficient Key Mechanisms in Multi Node Network for Secured Data Transmission", Int. J. Eng. Sci. Technol. Vol. 2, No. 5, 2010.
[22] A. Dogan, S. Berna and G. Saldamli., "Analyzing and Comparing the AES Architectures for their Power Consumption, Springer, 2014, pp. 263–271.