Improved Access Control Mechanism in Encrypted Cloud Data

Arivumathi I[1] Ms. Niranjana A[2]
[1]P.G. Student [2]Assistant Professor
[1]Department of Computer Science & Engineering [2]Department of Information Technology
[1,2]Kongunadu College of Engineering and Technology, Thottiam, Trichy, Tamil Nadu, India

***Abstract* - Mobile devices are rapidly becoming a key computing platform and an essential part of human life as the most effective and convenient communication tools not bounded by time and place. With the rapid growth of mobile devices and mobile applications, the need for mobile security also has increased dramatically. Due to increasing use of mobile devices the requirement of cloud computing in mobile devices arises, which gave birth to Mobile Cloud Computing. Mobile Cloud Computing refers to an infrastructure where data storage can happen away from mobile device i.e. on a cloud. To ensure the correctness of users' data in the cloud, the framework mainly focuses on the data security over the Cloud Computing Paradigm by purposing new cryptographic technique named as three tier architecture that includes SHA algorithm, Advance encryption standard algorithm and Elliptic curve cryptography algorithm. And also authenticate the users using cued click points in mobile environment. These algorithms can be implementing in real time mobile cloud environment and an experimental result proves with minimal performance degradation.**

Keywords: Mobile cloud computing, Cryptographic approach, Secure storage network, Hash functions, Cued points

INTRODUCTION:

Mobile devices are increasingly become an important part of human life as efficient and convenient communication tools are bounded by time and place. Mobile users use various rich services from mobile applications which can be run on the devices and/or on remote servers via wireless networks. The rapid development of mobile computing (MC) happens to a great trend in the progress of IT technology as well as commerce and industry fields. However, the mobile devices are opposite to many challenges in their resources and communications. The limited possessions noticeably delay the improvement of service characters. Cloud computing has been widely familiar as the next generation's computing infrastructure. CC offers some compensation by allowing users to use infrastructure, platforms, and software. Mobile cloud computing is defined as follows: "Mobile Cloud Computing at its easy refers to an infrastructure where both the data storage space and the data dispensation happen outside of the mobile device. Mobile cloud applications shift the computing power and data storage space away from mobile phones and into the cloud, bringing applications and mobile computing to not just Smartphone users but a much broader range of mobile subscribers".

RELATED WORK:

Hsiang Lu et.al…, [1] suggest that cloud computing be able to potentially save energy for mobile users. However, not all applications are energy efficient when migrate to the cloud. Mobile cloud computing services would be significantly dissimilar from cloud services for desktops because they must offer energy savings.

Ayesha Malik, et.al…, [3] analysis to give a solution for the threats that are the major topic for anyone when they want to accept cloud services for their work. For this purpose, a framework should be intended for execution of data and information securely in cloud environment. It will protect users' data, messages, information against various attacks.

Shashi Mehrotra Seth et.al…, [4] provide comparative survey for encryption algorithms that includes RSA, DES and AES algorithm. Supported on the text files are used. The experimental result it was concluded that DES algorithm devour least encryption time and AES algorithm has slightest memory usage even as encryption time difference is very minor in case of AES algorithm and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

THREE TIER MCC SECURITY

Individuals and enterprises obtain advantage to store enormous amount of data of applications on a cloud. However, problems are integrity and authentication.

Integrity: Every mobile cloud user must certain the veracity of their data stored on the cloud. Every access they create must be authenticated and verified. Different approaches in save integrity for one's information that is accumulating on the cloud is to be proposed. Example, every information stored up by every individual or enterprise in the cloud is labeled or analyzed to them wherein they are the single one to have access such information. Every access they make must be authenticated assuring that it is their own information and thus verifying its integrity.

Authentication: Different authentication methods have been presented and planned using cloud computing to secure the data access appropriate for mobile environments. Some employ the open standards and even ropes the integration of various authentication methods. For example, the use of contact or log-in IDs, passwords or PINS, authentication requests, etc.

Digital rights management: Illegal distribution and isolation of digital contents such as image, audio, video, and e-book, programs become more and more popular. Some solutions to defend these contents from illegitimate access are applied such as stipulation of encryption and decryption keys to contact these stuffing. A coding or decoding platform must be completed before any mobile user is able to have access to such digital contents. These terms are examined our proposed system and to provide MD5, AES and ECC algorithms for construct secure framework.

MD5: it is cryptographic hash function with 128 bit hash value practice a variable length message into fixed length output of 128 bits. The input message is broken into chunks of 512 blocks the message is padded so the length is divided by 512 bits. The sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

AES: The Advanced Encryption Standard (AES) identifies a cryptographic algorithm that can be worn to guard electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher-text; decrypting the cipher-text exchange the data reverse into its original form, called plaintext. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each of cipher has a 128 bit block size, with various key sizes of bits such as 128, 192 and 256 bits respectively.

RSA ALGORITHM:

The purpose of this page is to demonstrate step by step how a public-key encryption system works. We use the RSA algorithm (named after the inventors Rivest, Shamir, Adleman) with very small primes. Working with a public-key encryption system has mainly three phases:

Key Generation: Whoever wants to receive secret messages creates a public key (which is published) and a private key (kept secret). The keys are generated in a way that conceals their construction and makes it 'difficult' to find the private key by only knowing the public key.

Encryption: A secret message to any person can be encrypted by his/her public key (that could be officially listed like phone numbers).

Decryption: Only the person being addressed can easily decrypt the secret message using the private key.

PROPOSED THREE TIER FRAMEWORK:

When using the secure cloud storage services on resources limited Mobile Devices, the confidentiality of sensitive data must be ensured before uploading the data on cloud storage servers. The complex security operations to ensure security are restricted to execute due to the resource constrained mobile devices. The huge volume of complex security operations are offloaded remotely on cloud storage. By literature review of existing security frameworks focus on reducing the complexity of cryptographic algorithms or methods to offer confidentiality and security. By keep in view the requirements of security and privacy of confidential data of users with resource restricted mobile devices, in this paper, we present a proposed security framework for mobile cloud computing. In this framework the cryptographic methods as well as algorithms are used for encryption and decryption of mobile user data. This Framework ensures the additional security and confidentiality of user's sensitive or significant data. The flow of proposed work is illustrated in fig 1.

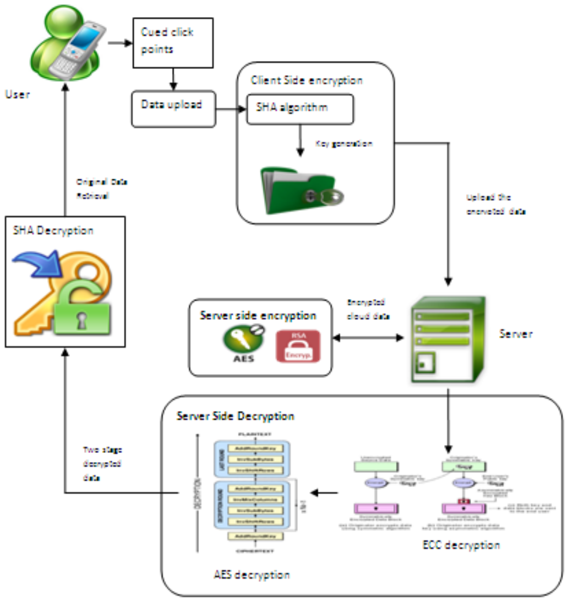


Fig 1: Proposed work

Cued click points:

The Cued Click Points (CCP) scheme is a proposed alternative to Pass-Points. In CCP, users click on one point on each of c = 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. Each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click.

SECURE HASH ALGORITHM:

- SHA was designed by NIST & NSA and is the US federal standard for use with the DSA signature scheme (nb the algorithm is SHA, the standard is SHS)
- it produces 160-bit hash values
- SHA overview
  - pad message so its length is a multiple of 512 bits
  - initialize the 5-word (160-bit) buffer (A,B,C,D,E) to
  - (67452301,efcdab89,98badcfe,10325476, c3d2e1f0)
  - process the message in 16-word (512-bit) chunks, using 4 rounds of 20 bit operations each on the chunk & buffer
  - output hash value is the final buffer value
- SHA is a close relative of MD5, sharing much common design, but each having differences
- SHA has very recently been subject to modification following NIST identification of some concerns, the exact nature of which is not public
- current version is regarded as secure

Step 1: Append Padding Bits….

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512.

Step 2: Append Length....

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 3: Prepare Processing Functions….

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)

f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)

f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)

f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

Step 4: Prepare Processing Constants....

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999	(0 <= t <= 19)
K(t) = 0x6ED9EBA1	(20 <= t <= 39)
K(t) = 0x8F1BBCDC	(40 <= t <= 59)
K(t) = 0xCA62C1D6	(60 <= t <= 79)

Step 5: Initialize Buffers….

SHA1 requires 160 bits or 5 buffers of words (32 bits):

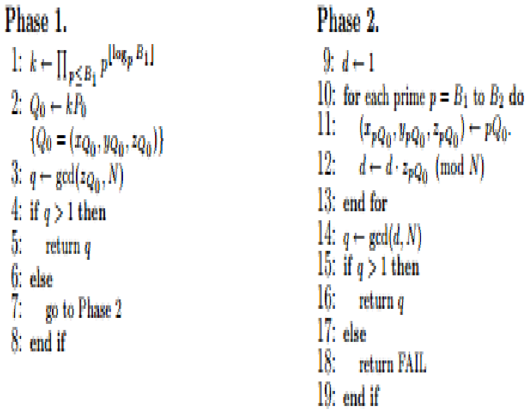
H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0

The basic flowchart as

Elliptic Curve Cryptography (ECC):

Elliptic curve is in the form of finite fields and provide fixed number of cipher text length.

Require: N: composite number to be factored,
E: elliptic curve,
$P_0 = (x_0, y_0, z_0)$
$\in E(Z_N)$: initial point, B_1: Smoothness bound for phase 1,
B_2: smothness bound for phase 2, $B_2 > B_1$



```
Phase 1.
$k \leftarrow \prod_{p \le B_1} p^{\lfloor \log_p B_1 \rfloor}$
$Q_0 \leftarrow kP_0$
    $\{Q_0 = (x_{Q_0}, y_{Q_0}, z_{Q_0})\}$
$q \leftarrow \gcd(z_{Q_0}, N)$
if $q > 1$ then
    return $q$
else
    go to Phase 2
end if

Phase 2.
$d \leftarrow 1$
for each prime $p = B_1$ to $B_2$ do
    $(x_{pQ_0}, y_{pQ_0}, z_{pQ_0}) \leftarrow pQ_0$.
    $d \leftarrow d \cdot z_{pQ_0} \pmod N$
end for
$q \leftarrow \gcd(d, N)$
if $q > 1$ then
    return $q$
else
    return FAIL
end if
```

Experimental results

The proposed work is to provide the secure mechanism for file upload and hosting services thus the additional resource consumption and the requirements are evaluated in these sections. The evaluated performance parameters are reported as:

Response Time: The amount of time required to accept the user request and get respond by the server is given as the response time of the system. The experimental result is showed in fig 2.

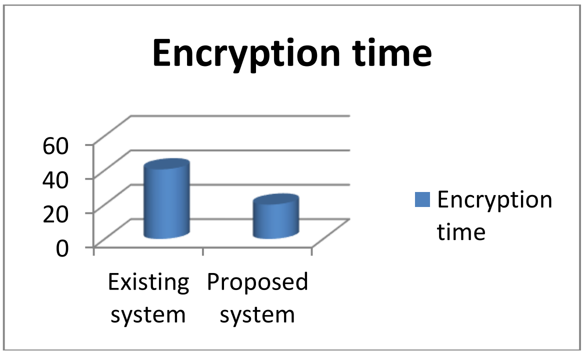


Fig 2. Response time

Space overhead The amount of data increases during the file encryption and the data transmission is given as the space overhead. That is evaluated in terms of KB (kilobytes) and reported using the below figure 4.

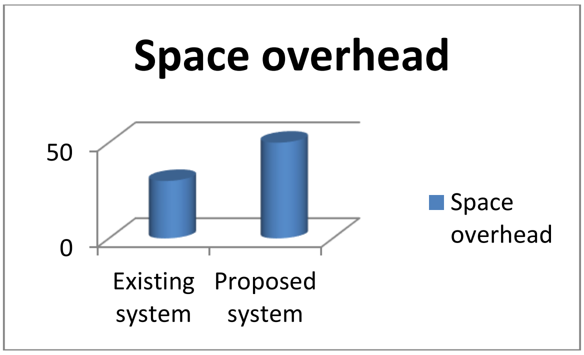


Fig 3. Space overhead

Encryption Time The amount of time required to encrypt or decrypt an input file is known as the encryption time of the system. The encryption time of the system is measured in terms of seconds and reported in the below figure 5.

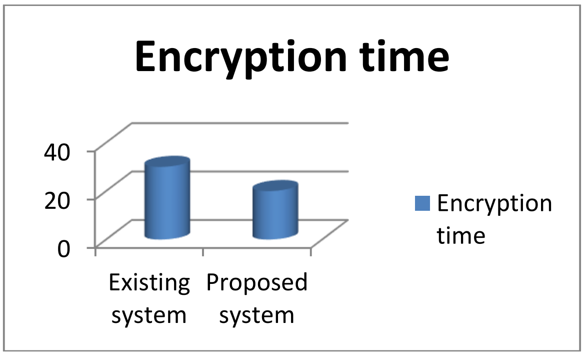


Fig 4: Encryption time

6. CONCLUSION

In this paper, we implemented a secure data mechanism to solve the problem of data security and privacy in mobile cloud computing. We can implement cued click point approach to provide the user authentication in mobile user side and implemented SHA algorithm to realize the access control in cloud computing, and show that the situation when mobile users may arbitrarily join or leave the mobile network makes these approaches not suitable to be used in mobile cloud computing. Afterwards, in this paper we explored AES-encryption scheme to make mobile users easily encrypt the data which are uploaded in cloud system. Then ECC algorithm is implemented successfully and experimental results proved reduced number of response time, space overhead and encryption time.

REFERENCES

[1] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review," Journal of Emerging Trends in Computing and Information Sciences, 2012.

[2] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication," IJCST Vol. 2, June 2011.

[3] Simoens, P., De Turck, F., Dhoedt, B., Demeester, P "Remote Display Solutions for Mobile Cloud Computing" Computer Vol.44 No.8,2011 pp.46–53

[4] Shahryar Shafique Qureshi1 , Toufeeq Ahmad1, Khalid Rafique2, Shuja-ul-islam3 "Mobile cloud computing as future for mobile applications – implementation methods and challenging issues" , 2011.

[5] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. "A Survey of Mobile Cloud Computing: Architecture Applications, and Approaches", In Wireless Communications and Mobile Computing 2011.

[6] Kumar, K., Lu, Y.-H.: Yung-Hsiang Lu, "Cloud Computing for Mobile Users" Can Offloading Computation Save Energy? Computer, Vol. 43, No.4, 2010 , pp.51– 56 .

[7] Mell P, Grance T "The NIST definition of Cloud Computing "NIST, Special Publication pp.800–145, Gaithersburg, MD

[8] Zhang Q, Cheng L, Boutaba R " Cloud Computing: state-of-the-art and research challenges" Journal of Internet Services Applications Vol.1 No.1 , 2010, pp. 7–18

[9] Pearson, S., Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing", in Proceedings of the 1st International Conference on Cloud Computing , Springer-Verlag: Beijing, China,2009, pp. 90-106.

[10] Wang, Q., et al., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", in Computer Security – ESORICS 2009, M. Backes and P. Ning, Editors, 2009, Springer Berlin / Heidelberg , pp. 355-370.