Suresh Gyan Vihar University International Journal of Environment, Science and Technology
Volume 1, Issue 1, 2015, pp. 92-100
ISSN:2394-9570

EFFICIENCY ANALYSIS OF SYMMETRIC ALGORITHMS FOR DATA SECURITY IN MOBILE CLOUD COMPUTING

Vijay H. Kalmani[1*] Sanjay Singla[2]
[1]*Research Scholar, School of Engineering & Technology, Suresh Gyan Vihar university, Jaipur - 302025, India*
[2]*Dean and Professor, Dean School of Engineering & Technology, IET Bhaddal Technical Campus, Ropar, Punjab,*
**Corresponding Author, email: vijaykalmani@gmail.com*

ABSTRACT

There are vast numbers of users who use cloud services through mobile devices such as mobiles, PDA, tablets, laptops due to its portability feature. Mobile Cloud Computing has many advantages inherent in it, but yet there are several risks and constraints exist, for e.g. security, data access control, efficiency, bandwidth, etc. Many cryptographic algorithms are studied prior to provide secured and efficient operations on web and standalone applications but very little research is done on symmetric algorithm implementation on mobile environment. To analyze the efficiency of various well known cryptographic security algorithms such as AES, DES and 3DES, these symmetric algorithms were implemented on mobile environment and through the results derived from real time implementation of these algorithms on various handheld devices, it is shown that which cryptographic technique can provide efficient and reliable security mechanism for data access control and security of user's outsourced data in mobile cloud computing.

Key Words: Mobile Cloud Computing, Key Management, Security, Cryptography

INTRODUCTION

Mobile Cloud Computing is an emerging technology and its popularity is increasing drastically day-by-day. Already a huge amount of population has accepted it for their various personal and commercial uses and the counting is still incrementing. Normally Mobile Cloud storage facilities users to distantly outsource their data and have the benefit of on-demand high quality cloud apps with no trouble of having local hardware and software tools. Although the advantages are understandable, such a service is also taking up users 'physical control' of their outsourced information, which unavoidably creates new safety threats towards the accuracy of the information in cloud. To start working on data access control, initially a thorough study is necessary to find out efficiency of cryptographic algorithms so that data operations on mobile could be fast and reliable.

User mobility, that means "anytime, anywhere" is turning in to an actuality. Making use of mobile tools, computing authority from cloud computing technology and Internet convenience jointly is making a new surge, which is mobile cloud computing for organizations. The utilization of mobile tools to set up ad-hoc communication method is a feasible solution that furnishes worldwide connectivity to

maintain a wide range of apps. Mobile cloud is a device-to-device service model, where a mobile device could utilize the cloud for storing, searching, data mining and multimedia processing. Cloud computing comes with several advantages such as, due to high resource availability on cloud servers, mobile users need not worry to have very high configuration devices with them for efficiency and power performance also CSPs provide resources in rental basis and are much more economical than buying expensive hardware. As user need to pay as per usage and range of hardware chosen so it is scalable and user can limit their resources to make it under their budget. The best part here is its global availability due to data storage on server side and accessibility over internet. User need not carry a particular device to access the service as nothing gets stored in their personal device. Also User need not take any burden of hardware servicing or maintenance or pay any extra maintenance charges. These things are routine tasks of CSPs and they do it without putting any burden on user. There are 'n' numbers of application which help in better organization of data or easy operations. These applications comes in packages and most of them are provided free of cost to the users for their convenience.

Despite these advantages, outsourcing of data on cloud environment suffers from various drawbacks too such as Data security risk; user need to outsource their private data to untrusted server and this could posses multiple security threats to the data from server admin and hackers. As cloud servers provide server access through http URL so internet connectivity is must for mobile users to connect to servers. User doesn't have physical possession of data and there is always risk on data consistency, thus it is always preferred to keep backup of data outsourced on server. Key management is another vast area of research and still studies are going on to make key management more secured and efficient.

Let us in brief have a discussion regarding the security problems that take place with key management on mobile devices with outsourcing data on cloud server. Common security problems in key management are

a. Efficiency in mobile operations
b. Strong security of cryptographic algorithms
c. Keys being fetched
d. Keys being susceptible to hack or compromise
e. Administration of all keys
f. Requires to measure linearly to manage many keys
g. Permitting approved user's access to their information

RELATED WORK

The authors [Yu *et al*. 2010] have demonstrated a measurable and well-grained data access control method in cloud computing on the basis of KPABE method. The data owner makes use of random key to encrypt a file, where the

random key is additional encrypted with a group of attributes by means of KP-ABE. After that, the group administrator allocate an access outline and the matching undisclosed key to approved users, such that a user could only decrypt a cipher content if and only if the data file attributes suit the access outline. So as to get user revocation, the administrator delegate's responsibilities of data file re-encryption and user undisclosed key revise to cloud servers.

On the other hand, the single holder approach possibly will hold back the execution of applications with the circumstances, where any associate in a group must be permitted to save and distribute data files with others.

In [Kallahalla *et al*. 2003] recommended a cryptographic storage method that facilitates protected file distribution on unreliable servers, called Plutus. With splitting files into file sets and encrypting each one file set with an exceptional file-block key, the data holder is able to share the file sets with others via dispatching the matching lockbox key, where the lockbox key is employed to encrypt the file-block keys. On the other hand, it results in an intense key sharing overhead for major file distribution. Furthermore, the file-block keys required to be revised and shared once more for a user un-authorization.

The authors [Lu *et al*. 2010] recommended a safe attribution method o the basis of code text-strategy attribute-oriented encryption method [B. Wang *et al*. 2012] that permits any associate in a group to distribute data with others. On the other hand, the concern of user un-authorization is not highlighted in their method. The authors [Yu *et al.* 2010] demonstrated a measurable and well-grained data access management method in cloud computing on the basis of key policy attribute-based encryption (KP-ABE) method [C. Wang *et al.* 2010]. Regrettably, the single possessor approach holds back the execution of their plan into the case, where any user is approved to preserve and distribute data.

A number of safety scheme for data distribution on unreliable servers have been recommended [M. Kallahalla *et al.* 2003, E. Goh *et al.* 2003, G. Ateniese *et al.* 2005]. In these systems, data holders preserve the encrypted data files in unreliable storage and share out the matching decryption keys merely to approved users. As a result, illegal users and storage servers not be able to find out the text of the data files. On the other hand; the difficulties of user involvement and un-authorization in these methods are linearly augmenting with several data holders and many retracted users, respectively.

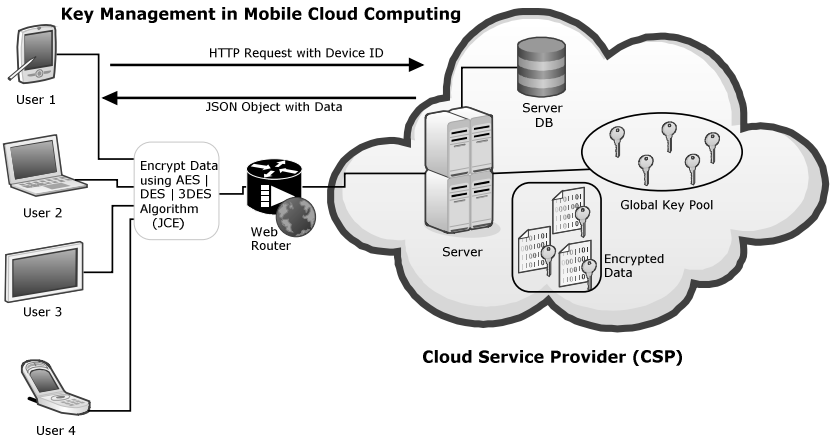

Figure 1: Architecture

METHODOLOGIES

Mobile environment has certain constraints in many aspects such as, low processing speed due to h/w constraint, works on battery power, consume airtime and low bandwidth. In order to design a system which can tackle these constraints we keep few objectives while planning methodology such as, minimal overhead should be on mobile for computation, consumption of battery should be very less, airtime should reduce due to fast communication, bandwidth saving due to only required data transmission and flexibility, so that single sign in should be enough.

Intend of this research is to study the efficiency of major symmetric cryptographic algorithms after implementing it on mobile environment. The most common and popular symmetric algorithms such as AES, DES and 3DES are taken into consideration as these algorithms are highly secured and studied much on standalone and web application but still research has to be done on mobile environment.

CSP (Cloud Service Provider) allows users to store or access their data in its cloud server. User can access the cloud services for outsourcing their data and operating on it using their mobile device. Mobile devices such as Mobile, PDA, Palmtop, Laptop have serial ID (Alternates are IMEI (Calling)/ OSid (Android) / Mac ID) but serial ID is common for all. Initially user need to register themselves using their device which will be used thereafter for further transactions. Serial number of device should be retrieved at the time of registration and sent to the server along with other details. Server stores serial number in hash code format in its database using SHA-1 algorithm. Device serial number will be mailed to the user for their future reference. Whenever user login, their device s/n hash code is checked with hash code present in server db. If verified

then a new session is created and their device serial number, whenever user outsource any data then encryption happen in their device itself through the serial ID as a key for AES, DES or 3DES algorithm and encrypted data gets stored in server. At the time of decryption server sends the encrypted data to the user and the same serial ID is used for decryption purpose. If user changes the device in future then they need to provide old serial ID which would be there in their mailbox and get 2 options to change the serial key temporary for current session or forever. For temporary i.e. current session then operations happen with old serial key only for encryption or decryption. if permanent then all the user data present in server db is decrypted using old serial and again gets encrypted using new serial. New serial hash code is replaced in database by old hash code.

Consideration of AES, DES and 3DES algorithm for mobile data security was taken after a brief research on their design and security features.

a. AES ALGORITHM

Advanced Encryption Standard (AES) stands on a rule acknowledged as a substitution-permutation system, amalgamation of both replacement & permutation, also is speedy in both s/w and h/w. Dissimilar to its ancestors DES, AES never utilize a Feistel system. AES is a type of Rijndael that has an unchanging chunk size of 128 bits as well as key size of 128, 192, or 256 bits.

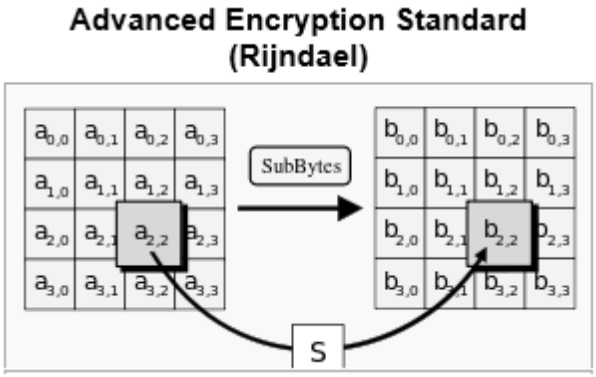

Figure 2: Advanced Encryption Standard (Rijndael)

AES works on a 4 by 4 column-major arrangement matrix of bytes, though some verities of Rijndael contain a larger chunk size and has extra columns in the state. Mainly AES computations are performed in an unusual finite field. The key size utilized for an AES code denotes the no. of recurrences of conversion rounds that transform the input, called the plain text, into the ultimate outcome, called the cipher text.

b. DES ALGORITHM

Data Encryption Standard (DES) is a symmetric chunk of secret-code implemented by IBM. DES utilizes a 56-bit key to encode/decode a 64-bit chunk of message. The key at all the times kept as a 64-bit chunk, every 8th bit of that is overlooked. Yet, it is common to place every 8th bit so that every set of 8 bits has an odd no. of bits places to 1.

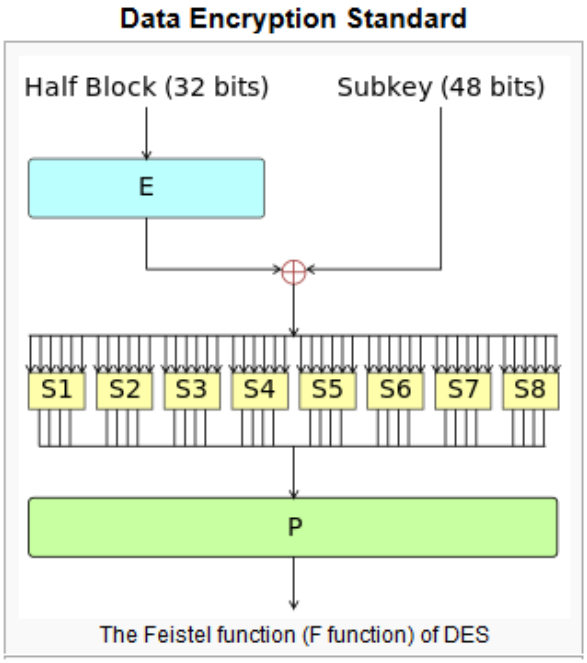

Figure 3: Data Encryption Standard

This cryptographic standard is paramount to implement in h/w, perhaps to it can be implemented in applications as well, but compared to hardware, operations takes more time in software. Though, contemporary computing devices are so speedy that we get pleasing results.

c. 3DES ALGORITHM

In cipher science, 3DES is the familiar term for the Triple Data Encryption Algorithm (TDEA) symmetric-key chunk cipher texts that use the DES cipher text algorithm 3 rounds to individual data chunks. The primitive DES cipher text's key size of 56 bits was usually enough when that algorithm was developed, but the accessibility of advanced technologies made brute-force vulnerable to the system.

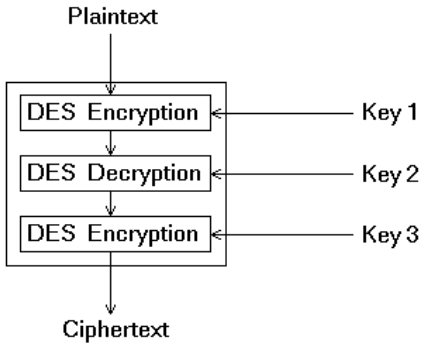

Figure 4: Architecture of 3DES

3TDES offers a comparatively easy way of mounting the key size of DES to defend from such vulnerabilities, with no requirement to design a totally new block encoding mechanism.

IMPLEMENTATION

Main objective of this study was to design an architecture where data owner can outsource their data through mobile device with high efficiency and security. The main algorithms considered here were AES, DES and 3DES. All three algorithms were implemented on android language and were run on mobile devices to check the efficiency of these symmetric algorithms. For performance measures 3 different mobile devices were used of diverse configurations. Device configurations are as follows:

Specifications	Samsung Galaxy Tab 3 (Device 1)	Samsung Galaxy Star Trios (Device 1)	Samsung Galaxy S Duos 2 (Device 1)
OS	Android v4.1.2 (Jelly Bean)	Android v4.1.2 (Jelly Bean)	Android v4.1.2 (Jelly Bean)
Chipset	Marvell PXA869	Qualcomm MSM7225A Snapdragon	BCM 28145/28155
CPU	Dual-core 1.2 GHz Cortex-A9	1 GHz Cortex-A5	Dual-core 1.2 GHz Cortex-A9
GPU	PowerVR SGX540	Adreno 200	Broadcom VideoCore IV
Memory	16 GB, 1 GB RAM	4 GB, 512 MB RAM	4 GB, 768 MB RAM

Table 1: Device Configurations

For the purpose of data storage on server Google's cloud storage service was considered were every encrypted data was being stored to the server.

EXPERIMENTAL RESULTS

Extensive experiments were conducted to check efficiency of symmetric algorithms on mobile environment for encryption and decryption of data before outsourcing data to cloud servers. Experiments revealed performance of algorithms i.e. AES, DES and 3DES when executed for diverse no. of operations simultaneously. Below are the results of algorithm performance which were found in study:

A. *Device Performance on Algorithms*

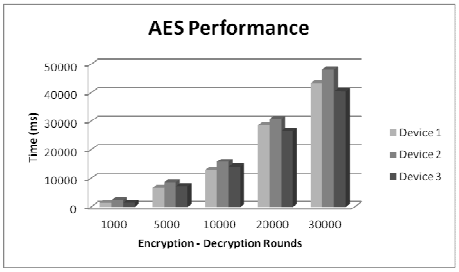

Figure 5: AES Performance

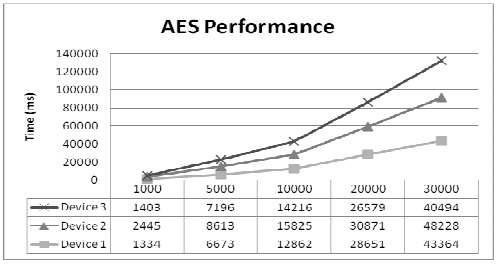

Figure 6: AES Performance

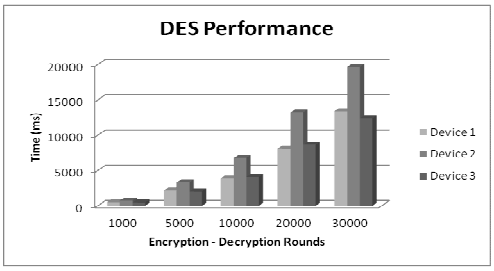

Figure 7: DES Performance

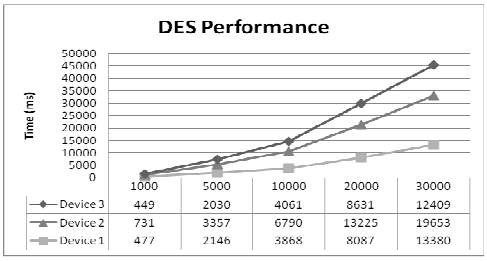

Figure 8: DES Performance

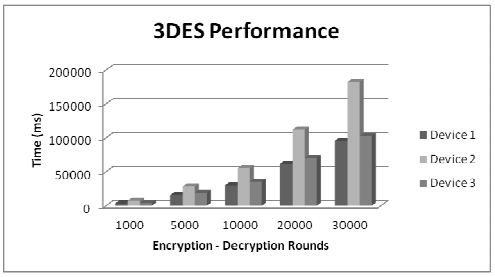

Figure 9: 3DES Performance

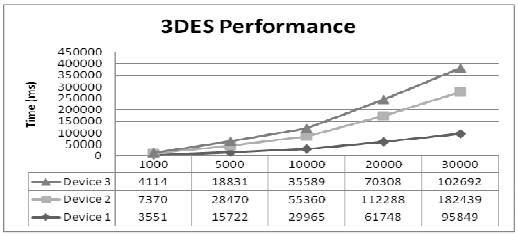

Figure 10: 3DES Performance

B. *Algorithm Performance on Devices*

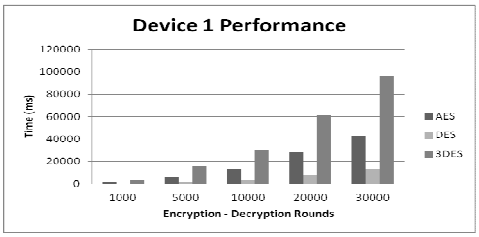

Figure 11: Device 1 Performance

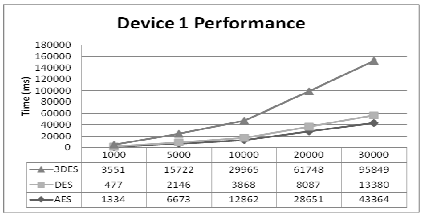

Figure 12: Device 1 Performance

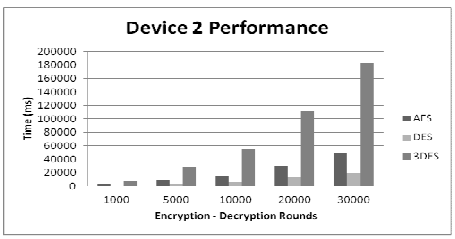

Figure 13: Device 2 Performance

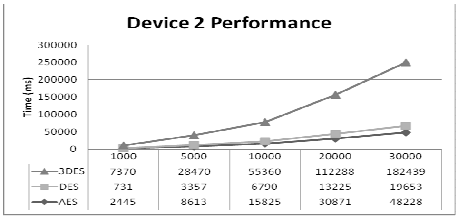

Figure 14: Device 2 Performance

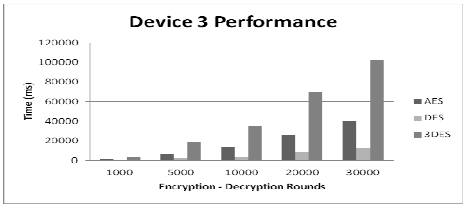

Figure 15: Device 3 - Performance

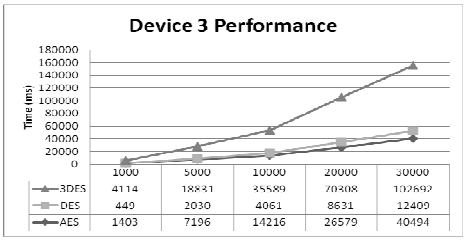

Figure 16: Device 3 Performance

CONCLUSION

Having a deep study on performance of 3 major symmetric algorithms i.e. AES, DES and 3DES on android based mobile devices for data outsourcing on cloud, it is concluded that performance of DES is far better than other 2 algorithms in case of efficiency and throughput. Performance of 3DES on security scale is not comparable to AES and DES as 3DES takes as much as 3 times more processing time than DES but the same time it provides 3 times stronger security than DES algorithm. For an optimum level of efficiency and security even AES can be

recommended as its efficiency is better than 3DES and security wise it is comparable to DES. DES is considered to be quiet weak among these 3 algorithms in previous researches. As mobile devices lack in high resource compared to desktops and laptops, it can be generalized that AES may prove to be a good option to implement on mobiles for better performance and security.

REFERENCE

S. Yu, C. Wang, K. Ren, and W. Lou. 2010. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. *Proceeding IEEE INFOCOM* : 534 –542.

M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, 2003. Plutus: Scalable Secure File Sharing on Untrusted Storage. *Proceeding USENIX Conf. File and Storage Technologies*: 29–42.

E. Goh, H. Shacham, N. Modadugu, and D. Boneh. 2003. Sirius: Securing Remote Untrusted Storage. *Proceeding Network and Distributed Systems Security Symp.* (*NDSS*) : 131–145.

R. Lu, X. Lin, X. Liang, and X. Shen. 2010. Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing. *Proceeding ACM Symp. Information, Computer and Comm.Security* : 282-292.

G. Ateniese, K. Fu, M. Green, and S.Hohenberger. 2005. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. *Proceeding Network and Distributed Systems Security Symp. (NDSS)* : 29-43.

B. Wang, B. Li, and H. Li. 2012. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud. *Proceeding 10th Int'l Conf. Applied Cryptography and Network Security* : 507-525.

C. Wang, Q. Wang, K. Ren, and W. Lou. 2010. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. *Proceeding IEEE INFOCOM:* 523-533.