Mobile Storage protection during Encryption Algorithm

Dr. P.Geetha
Assistant Professor
Department of Computer Science, Dr.URCW, Karaikudi.

***Abstract* - Mobile Computing promotes uses of cloud based services in a portable environment. With the fast growth of mobile application, mobile security is predominately needed. To make sure the accuracy of User's information in the cloud, the method generally focuses on the data protection over cloud computing paradigm. Many encryption technique have been proposed for secure communication. This paper presented the characteristics of a mixture of encryption algorithms with their limitations. Comparative analysis has been reviewed based on different size of records slab to estimate encryption/ decryption speed.**

Key terms: Encryption, decryption, Security, Cloud storage, Mobile Device

I. Introduction

The mobile computing is the emerging area of Information and CommunicationsTechnology (ICT). Mobile users is still increasing due to constantly improving user friendly hardware and software of mobile devices. Now adays, the smartphones and tables are used to share emailing, chatting, browsing, file sharing, reading or editing documents,entraining etc. From the market analysis, it was predicted that the number of usage of mobile devices is constantly increasing globally [3]. However, the mobile computing alone fails to meet the full satisfaction of the large number of users and their computational requirements.

The mobile cloud computing (MCC) is introduced as services of cloud computing, which is offered in either mobile phone environment or mobile embedded system environment. Mobile computing is integrated with cloud computing because of the essential characteristics of cloud model such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. Moreover, the cloud computing is being popular to the mobile users as it can provide cloud like services [4], [5].

The mobile computing is used to demonstrate, development, transfer and distribute the applications and resources, whereas wireless communication is used so that the mobile users can utilize the network resources, services and support the communication between mobile devices and clouds.

II. Elucidation of various Encryption Algorithms

The proposed method compared three encryption techniques like AES, DES and RSA algorithm with their combination, namely A-RSA and D-RSA. DES and AES belong to symmetric key cryptography and RSA belongs to asymmetric key cryptography. RSA can be used only to encrypt small data and cannot be used for large data. But in AES and DES adopting longer key generation for avoiding these complexities, best solution to use RSA for bulk data encryption using the comparison of a secret key and public key based ARSA and DRSA algorithms. It solves the problem of key agreement and key exchange problem generated in secret key cryptography.

The detailed explanations of these techniques are explained below. Experimental analyses are given for evaluating the effectiveness of each algorithm. The main concern of cryptography technique is Security and Privacy which protect the data against attacks with less time consuming.

AES

Advanced Encryption Standard [AES] is a symmetric key cryptography technique that encrypts data blocks of 128 bits using symmetric keys of the size 128,192 (or) 256 accordingly uses 10,12 or 14 rounds. AES uses transformation types for providing security and speed.

DES

Data Encryption Standard [DES] is a symmetric block cipher that encrypts 64 bit block size with 56 bit key. It consists of 16 rounds of performing permutation and substitution. It provides a standard method for protecting sensitive and commercial data. Here same key is used for encryption and decryption.

RSA

It is a public key designed by Ron Rivest, Adi Shamir and Leonard Adleman. RSA operations can be decomposed into three steps such as key generation, encryption and decryption. The same key is used to encrypt the data for providing Security.

ARSA

Symmetric algorithm AES associated with RSA implemented for Security. During Encryption, private and public keys are generated using RSA then random AES key formed and encrypted through the RSA public key as well as data are encrypted through AES key and decryption is in reverse process[9].

DRSA

Symmetric algorithm, DES associated with RSA implemented for Security. During Encryption, private and public keys are generated using RSA then random DES key formed and encrypted through the RSA public key as well as data are encrypted through DES key and decryption is in reverse process[10].

III. Performance Evaluation of various Encryption Algorithms

In the following table, characteristics between AES, DES, RSA, ARSA and DRSA is presented with 8 factors such as key size, block size, the algorithm used, encrypted time, decrypted time, power consumption, security, keys used and rounds.Comparative analysis has been reviewed based on different size of data blocks & keys to evaluate encryption/ decryption speed. ARSA and DRSA combines AES and DES encryption algorithm respectively[10].

Characteristics	AES	DES	RSA	ARSA	DRSA
Security	Excellent	Not Secure	Least Secure	Excellent	Least Secure
Keys used	Same key used for Encryption &Decryption	Same key used for Encryption &Decryption	Different key used for Encryption &Decryption	Secret key used for Encryption &Decryption	Public key used for Encryption &Decryption
Key Size	256 bits	56 bits	>1024 bits	>1024 bits	>1024 bits
Block size	128 bits	64 bits	512 bits	512 bits	512 bits
Power Consumption	Low	Low	High	High	Low
Encryption	Faster	Moderate	Slower	Slower	Faster
Decryption	Faster	Moderate	Slower	Faster	Slower
Algorithm used	Symmetric	Symmetric	Asymmetric	Combined Symmetric & Asymmetric	Combined Symmetric & Asymmetric

IV. Conclusion

Encryption Algorithm plays a major role in Secure Communication whereas file size, time computing, power consumption is the major concern. The encryption techniques AES,DES and RSA with the combination ARSA, DRSA are used for evaluating the performance based on the usage of text files. It is clearly proven that ARSA provides better result in all aspects compared with various encryption algorithms.

References

[1] K.-Y. Chung, J. Yoo, and K. J. Kim, "Recent trends on mobile computing and future networks," Personal and Ubiquitous Computing, vol. 18, pp. 489-491, 2014.
[2] H. Ba, W. Heinzelman, C.-A. Janssen, and J. Shi, "Mobile computing-A green computing resource," in Wireless Communications and Networking Conference (WCNC), 2013 IEEE, 2013, pp. 4451-4456.
[3] [Online: 2016] A Report of Worldwide Smartphone Markets: 2011 to 2015, May 2011: http://www.researchandmarkets.com/research/7a1189/worldwide_smartphone
[4] M. B. Mollah, K. R. Islam, and S. S. Islam, "Next generation of computing through cloud computing technology," in Electrical & ComputerEngineering (CCECE), 2012 25th IEEE Canadian Conference on, 2012, pp. 1-6.
[5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems, vol. 25, pp. 599-616, 2009.
[6] [Online: 2016] ABI Research Report on Mobile Cloud Computing; ttps://www.abiresearch.com/research/product/1005283-mobile-cloudapplications/.
[7] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future Generation Computer Systems, vol. 29, pp. 84-106, 2013.
[8] E. Ahmed, A. Gani, M. K. Khan, R. Buyya, and S. U. Khan, "Seamless application execution in mobile cloud computing: Motivation, taxonomy, and open challenges," Journal of Network and Computer Applications, vol. 52, pp. 154-172, 2015.
[9] Sujithra.M , Padmavathi.G, "Ensuring Security on Mobile Device data with two Phase Algorithm over Cloud storage", Journal of Theoretical and Applied Information Technology,Vol 80 No. 2 2015.
[10] Nitin Nagar, Ugrasen Suman, "A Secure Mobile Cloud Storage Environment using Encryption Algorithm", International Joural of Computer Applications, Volume 140, no.8 April 2016.