Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.92 – 97

SURVEY ON CRYPTOGRAPHIC ALGORITHMS FOR OUTSOURCING MOBILE DATA TO CLOUD

S.Velmurgan
M.Phil. Scholar,
Department of Computer Science,
Bishop Heber College (Autonomous),
Trichirappalli, Tamilnadu, India

R.Thamarai Selvi
Asst. Professor & Head,
Department of computer Applications,
Bishop Heber College (Autonomous),
Trichirappalli, Tamilnadu, India

ABSTRACT: Mobile devices are fast becoming a key computing platform and an essential part of human life as the most effective and suitable statement tools not bounded by time and place. Mobile Cloud Computing refers to an infrastructure where data storage space can happen away from mobile device i.e. on a cloud. To ensure the correctness of users' data in the cloud, the framework essentially focuses on the data security over the Cloud Computing Paradigm by purposing new cryptographic technique named as Two Phase SHA and AES encryption algorithms to secure the files in the server and for increasing the transfer rate of the information the file is used. The performance of the secure technique is performed using the .NET technology and their performance in terms of time complexity and storage overhead computed. The results maintain the efficient methodology of file hosting and allotment in the cloud storage additionally that is efficient during the speedy upload and downloads. Thus the proposed technique is adoptable e and secure for secure storage services.

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

I. INTRODUCTION

Mobile cloud computing was form after the concept of "cloud computing", this was launched in mid of 2007. It has been grabbing the kindness of the entrepreneurs as a money making business option that minimizes the expansion process and the management cost of mobile applications of the mobile users as a latest technology to accomplish Wealthy experience of a selection of mobile services at low cost.

Mobile applications must be quickly provisioned and released with the work of negligible administration efforts or the service provider's communications. With the explosion of mobile applications and the provision of Cloud Computing for a range of services for mobile users, mobile cloud computing is introduced as an addition of cloud computing into the mobile location. But the major issue present in this technology is security of outsourced data as protection is main issue in cloud computing also. Security risks in Mobile Cloud Computing should be even more because we have to take care of cloud protection as well as mobile security.

Cloud computing is a universal term for anything that involve distributing hosted services over the Internet. These services are broadly separated in the three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), The Infrastructure as a Service (IaaS) the neutral infrastructure by a seller which you can contact more than internet and usage to install your software, build or install your applications. Infrastructure as a service (IaaS) is an identical, highly automated offering, where compute possessions, complemented by storage and networking capabilities are own and hosted by a cloud service provider and offered to customer on - demand.

1.1. TERMS OF CRYPTOGRAPHY

Plain Text: The unique message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual: letter that has to be send to the other end is given a special name as Plain Text.

Cipher Text: The message that cannot be understood by anyone or pointless message is what we call as Cipher Text. In Cryptography the unique message is transformed into non readable message before the transmission of actual message.

Encryption: A procedure of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption method to send confidential messages over an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. Encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

Decryption: A reverse procedure of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption scheme at the receiver side to obtain the original message from non-readable message. The process of decryption require 2 things- a Decryption algorithm and a key. A Decryption algorithm means the system that should be used in Decryption. Generally the encryption and decryption algorithm are same.

Key: A Key is a number or alpha numeric text or may be a special symbol. The Key is used at the moment in time of encryption take place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very significant since the security of encryption algorithm depends directly on it.

II. RELATED WORK

The authors [Yu *et al*. 2010] have established a assessable and well-grained data access control method in cloud computing on the basis of KPABE technique. The data owner makes use of random key to encrypt a file, where the random key is additionally encrypted with a group of attribute by means of KP-ABE. After that, the group administrator allocate an access outline and the matching unnamed key to users, such that a user could only decrypt a cipher content if and only if the data folder attributes suit the access draw round.

On the other hand, the single holder move toward probably will hold back the execution of applications with the difference circumstances, where any associate in a group can't be allowed to save and distribute data files with others.

In [Kallahalla *et al*. 2003] optional a cryptographic storage method that facilitates protected file distribution of changeable server, called Plutus. With splitting files into file sets and encrypting each one folder place through an excellent file-block key, the information holder is able to share the file set with the others via dispatching the similar lockbox key, where the lockbox key is working to encrypt the file block keys. On the other hand, it outcome in an strong key distribution overhead for major file sharing. Moreover, the file-block keys required to be reviewed and shared one or more for a user un-authorization.

A integer of safety scheme for data distribution on undependable servers have been recommended [M. Kallahalla *et al.* 2003, E. Goh *et al.* 2003, G. Ateniese *et al.* 2005]. Systems information holders preserve the encrypted data files in unreliable storage space and share out the same decryption keys only to approved users. As a result, illegal persons and storage space servers not be able to find out the text of the data files. On the other hand; the difficulties of user involvement and authorization in these method are linearly augment with several data holders and many retracted users, respectively.

The author [Lu *et al.* 2010] optional a safe attribution method o the basis of code text strategy attribute-oriented encryption technique [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 authorization is not decorated in their method.

The authors [Yu *et al.* 2010] establish 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]. Unfortunately, the single possessor approach holds back the execution of their plan into the case, anywhere any user is approved to preserve and distribute data and get the fully authorized data.

III. PERFORMANCE ANALYSIS

The Performance analysis can be taken three encryption techniques like AES, DES and RSA algorithms with their amalgamations namely ARSA and D-RSA. The DES and AES ideally belong to the category of symmetric key in cryptography and RSA belongs to the category of asymmetric key cryptography. The complete explanation of the proposed techniques is explained below. Experiments results are given to analysis the efficiency of each algorithm. There are two main features that specify and distinguish one algorithm from another are the capability to secure and protect the data against attacks and speed of encryption and decryption.

COMPARATIVE ANALYSIS

The following tables and graph shows the comparison between the existing system and the proposed system. The proposed system provides more number of properties as well as compare to existing system.

TABLE 1: Comparison Study with Existing System

Property	WWMO	GA	CT	THJ	IBSDDS	Previous Result
Unidirectional	YES	YES	YES	YES	YES	YES
Non-Interactive	NO	NO	YES	YES	YES	YES
Key optimal	YES	YES	YES	YES	YES	YES
Collusion-safe	YES	YES	NO	NO	YES	YES
Non-transitive	YES	YES	YES	YES	YES	YES
File-based access	NO	NO	NO	NO	YES	YES
Owner Convenient System	NO	NO	NO	NO	NO	YES
Offline Notifications as SMS	NO	NO	NO	NO	NO	YES
DDOS	NO	NO	NO	NO	NO	YES

TABLE 2 : Number Of Properties Applicable To Existing System

System	No. Of properties applicable
WWMO	4
GA	4
CT	4
THJ	4
IBSDDS	6
Proposed System	9

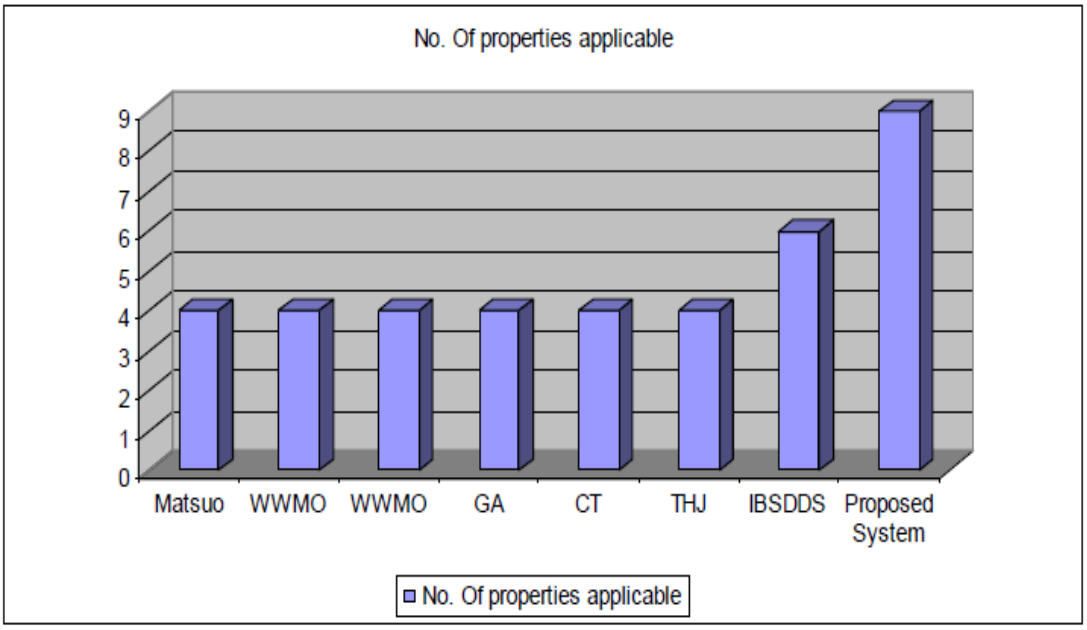

Fig 1.Graph for comparison of Proposed System and Existing System

SR NO.	File Name	File Type	File Size	Time (ms) Encryption	Reencryption	Decryption
1	server	txt	30KB	0	20	10
2	connect111	txt	338KB	16	20	40
3	machine	txt	1.34MB	40	70	60
4	client	txt	14.7MB	360	480	850
5	document	doc	22KB	10	10	20
6	Implementation	doc	165KB	10	10	25
7	v1	doc	1.16MB	70	10	70
8	Varsha REPORT	doc	9.25MB	190	10	530
9	VisaCard Platinum	xls	18KB	10	20	10
10	2013-14 TT	xls	165KB	10	10	10
11	Tg data comp	xls	523KB	30	20	30
12	FACULTY TT	xls	1MB	30	20	20
13	christmas fair	pdf	11KB	0	10	10
14	iiiij	pdf	158KB	10	15	30
15	Identity	pdf	1.07MB	20	30	60

Table 3 : Time Required For File Upload And Download In Milli Seconds

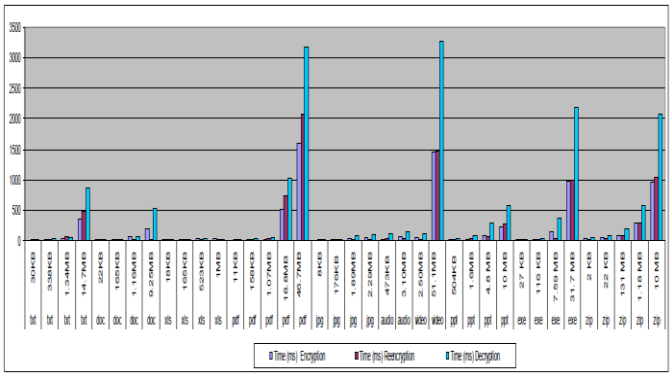

Fig 2.Graph of System results

IV. CONCLUSION

In this study Two Phase RSA encryption algorithm for protecting the confidentiality and integrity of uploading files or data in mobile storage cloud. Encryption algorithms play an important role in communication security whereas input data size, Computation time, power utilization and mean processing time are the major issue of concern. The selected encryption combinations A-RSA and DRSA algorithms are used for performance evaluation based on the text files used and the experimental result it was concluded that A-RSA algorithm gives better result in all aspects compared to D-RSA algorithm. Many more algorithms to be evaluate and their results can be analyzed with one another to produce the most excellent implemented security algorithm in cloud background for future use. This technique analyzes the range of the data security and encryption process was very high while comparing old technique.

REFERENCES

[1] PortioResearch,"Mobilesubscribersworldwide", *[online] Available www.onbile.comlinfo/mobile*.
[2] Morten V. Pedersen, Member IEEE, and Frank H. P. Fitzek, Senior Member, "Mobile Clouds: The New Content Distribution Platform", *Proceedings of the IEEE*, Vol. 100, May, 2012.
[3] M.Sujithra,G.Padmavathi,SathyaNarayanan,"Mobie Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud", *Procedia Computer science*, volume 47, pages 480-385, 2015.

[4] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S.Paraboschi, and P. Samarati, "A data outsourcing architecture combining cryptography and access control", *In Proceedings of the ACM workshop on Computer security architecture*, pages 63–69, 2007.
[5] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", *IEEE Students' Conference on Electrical, Electronics and Computer Science*, pp. 1-5,2012.
[6] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM* , Feb 1978.
[7] Wei Ren, Linchen Yu, Ren Gao, Feng Xiong," Light weight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing", *Tsinghua Science And Technology*,ISSNl1007-0214ll06/09ll,pp520 528.Volume 16, Number 5, October 2011.
[8] Itani W, Kayassi A, Chehab A "Energy-efficient incremental integrity for securing storage in mobile cloud computing", *International Conference on Energy Aware Computing (ICEAC10)*, Cairo, Egypt, 2010.
[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", *Proceeding IEEE INFOCO* , 534 –542, 2010.
[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q.Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage",. *Proceeding USENIX Conf. File and Storage Technologies*, 2003.
[11] E. Goh, H. Shacham, N. Modadugu, and D.Boneh, "Sirius: Securing Remote Untrusted Storage". *Proceeding Network and Distributed Systems Security Symp. (NDSS)* : 131–145, 2003.
[12] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance", *The Essential of Bread and Butter of Data Forensics in Cloud Computing.Proceeding ACM Symp. Information, Computer and Comm.Security* : 282-292, 2010.
[13] G. Ateniese,K. Fu,M. Green,and S.Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", *Proceeding Network and Distributed Systems Security Symp. (NDSS)* , 2005.
[14] B. Wang, B. Li, and H. Li.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, 2003.
[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", *Proceeding IEEE INFOCOM*, 523-533, 2010.

