Security Enhancement in Cryptography for Mobile Device Outsourced in Cloud Computing

Harihara Krishnan R, Aby John, A. Amali Asha, Venisha Leena Mary R

Abstract: Mobile devices often store data in cloud computing storage based on the increasing availability of the users. But security is the major issue in cloud computing. Sensitive information is stored and provided across internet to make sure that the data is protected with security. In this paper, the concept of data privacy is given more importance with regard to the major problem of reducing outsourced data usage. Mobile computing has memory storage and power resources as limitations. But cryptography is a concept which provides some sort of security enhancement that ensures the authentication and the availability of data integrity with confidentiality. Certain algorithms are used for ensuring an increase in security such as AES, DES, and Blowfish. Experimental results are computed and analyzed to level up the performance using cryptographic algorithms. Results are shown in order to assure resistance among the above techniques. Choosing an apt algorithm will quench the requirements of the future.

Keywords: AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish, Cryptography, Confidentiality, Integrity of data.

I. INTRODUCTION

A.CRYPTOGRAPHY

It is defined as changing a plain text into a cipher text; in other words, changing a normal text into some other different format. It is basically derived from mathematical concepts and secured information for communication. Such techniques are called algorithm. Security is the main feature in cryptography. For the data stored in cloud, cryptography is divided into three types. They are symmetric, asymmetric and having techniques for solving some issues in the security.

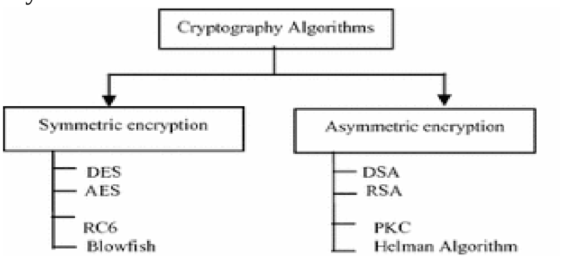

Figure 1.1 Types of Cryptographic Algorithms

Revised Manuscript Received on June 30, 2020.
* Correspondence Author

Harihara Krishnan R*, Research Scholar, Department of Computer Science, Presidency College (Autonomous), Chennai, India.

Aby John, Research Scholar, PG and Research Department of English, Presidency College (Autonomous), Chennai , India.

Dr. A. Amali Asha, Assistant Professor, Department of Computer Science, Loyola College (Autonomous), Chennai , India.

Venisha Leena Mary R, Research Scholar, Department of Computer Science, Periyar University, Salem 636 011.

Symmetric cryptography

For both encryption and decryption, the key used is same. Such a mechanism is known as secret key cryptography or symmetric cryptography. These types of mechanisms are used in AES, DES, Blowfish and RC5 algorithms.

Asymmetric cryptography

For both encryption and decryption, different keys are used. For RSA the same procedure is followed. Such type of mechanism is known as public key cryptography or asymmetric cryptography.

Hash Algorithm

Hash algorithm is also known as the message digest. Input data is recreated from hash value MD5, MD2, MD4, SHA1, SHA2, Whirlpool etc.

B. ISSUES IN THE SECURITY (CLOUD COMPUTING)

Security

The cloud data is stored with specific boundaries. Therefore, strong security encryption techniques are used for the third party.

Authentication

The origin of the message for proof of identities is used to ensure it. It correctly identifies the hometown.

Integrity

For both the sender and the receiver, message or the data remain the same. In order to check the correctness of the data that is stored in the cloud. Updating data violates the integrity of the same.

Confidentiality

The sender and the receiver can access the data. The basic principle of confidentiality is that the sensitive information is not being accessed by unauthorized process. Only cloud service provider knows whether the data is public or private and whether it can be accessed or not.

Data storage

For the ease of access, it provides data with multiple copies of the content. In order to overcome these problems, content stored in and across independent locations should be avoided.

Access control

It performs the action based on who access the data in the cloud. Non- repudiation sender cannot claim that the message is sent. It will not provide non-repudiation.

Availability

Cloud service provider always avail data to unauthorized persons of resources.

Laptop
Network
Smartphone
Cloud Computing
Tablet computer
Server
Mobile
Database

Figure 1.2 Cloud Environments for Mobile Device

II. II PROPOSED METHODOLOGY

C. DES

For encryption and decryption process, one secret key is used. The length of the key is 60 bits and encryption of a message it uses will be in 64 bits of size in block. Algorithm utilizes 60 bits directly and the input key is used as permutation nearly for 16 rounds till the final permutation gets over. DES is one of the most secured algorithms for large data. But length of the key used has some limitation.

Table 1.1 Comparisons of Symmetric Algorithms

Metrics	**DES**	**AES**	**BLOWFISH**
Structure	Feistal	Substitution Permutation	Feistal
Key Length	60	32-448	128,192,256
Rounds	16	10,12,14	16
Block Size	64	128	64
Through put	Less than AES	Less than Blowfish	Higher
Security	Adequate	Good	Very Good
Speed	Slower	Faster	Faster (High Speed)

D. AES

It is one of the secret algorithms in which the key is used as same for both encryption and decryption of data. When same key is used for both encryption and decryption, permutation of rounds are less compared to DES. Encryption is fast and effective for implementation. The length is 128,192 and 256 block size.

Table 1.2 Time Comparison for Encryption and Decryption

Algorithm	**File Size**	**Time Encryption (milliseconds)**	**Time Decryption (milliseconds)**
Blowfish	15KB	303	304
	25KB	315	313
	35KB	325	322
	40KB	330	324
	45KB	334	328
	55KB	339	330
	60KB	341	334
AES	15KB	306	307
	25KB	320	317
	35KB	326	323
	40KB	332	328
	45KB	338	333
	55KB	343	339
	60KB	347	342
DES	15KB	309	309
	25KB	318	318
	35KB	324	321
	40KB	331	326
	45KB	335	332
	55KB	342	339
	60KB	345	340

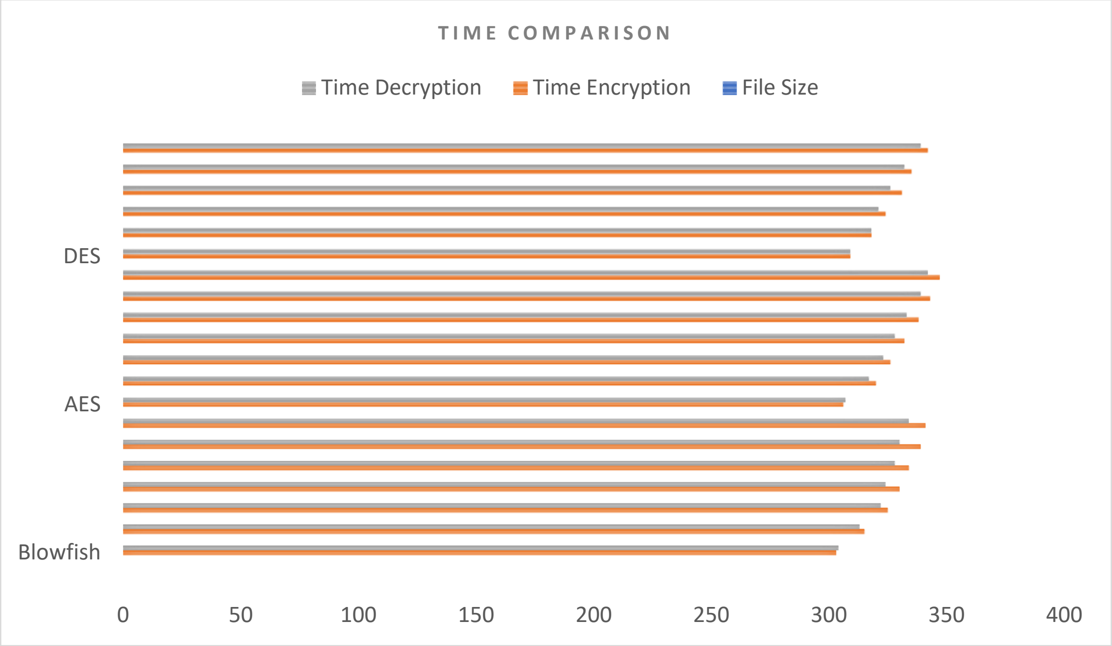

Figure1.3 Time Comparison -Encryption and Decryption

E. BLOWFISH

It is one of the fastest and freely available algorithms for encryption and decryption for alternating algorithms. Its key ranges from 32-448 and block size is 64 bits. Only for encryption, these algorithms use nearly 16 rounds. For each round the key and the data is dependent permutation and substitution is done. Sub key generation converts key up to 448 bit long to 4168. This type of algorithm is used only in smart phones because of its security level and speed with higher level.

Table1.3 CPU and Memory Comparison – Experimental Result

Algorithm	File Size	Encryption CPU%	Decryption CPU%	Encryption Memory KB	Decryption Memory KB
Blowfish	15KB	22.7	18.1	17.9	8.3
	25KB	20.2	18.8	17.6	17.4
	35KB	20.9	24.3	17.9	17.5
	40KB	21	24.4	18.0	17.7
	45KB	22.3	24.9	18.4	18.1
	55KB	22.5	25	18.7	18.3
	60KB	23.1	25.3	19.1	18.6
AES	15KB	25.3	23	20.5	20.3
	25KB	25	23.7	20.6	20.1
	35KB	26.2	32	21.7	21.7
	40KB	26.8	32.3	22.2	22.1
	45KB	27.2	33.3	23.1	22.9
	55KB	29.1	34.1	24.2	23.8
	60KB	29.8	34.3	25.3	24.3
DES	15KB	23.3	23.6	21.9	21.3
	25KB	25.3	26.7	23.9	22.9
	35KB	26.4	28.1	25.1	23.1
	40KB	27.2	28.4	25.9	24.2
	45KB	27.9	28.6	26.1	25.1
	55KB	28.7	29.1	27.5	26.2
	60KB	29.9	31.0	28.0	27.4

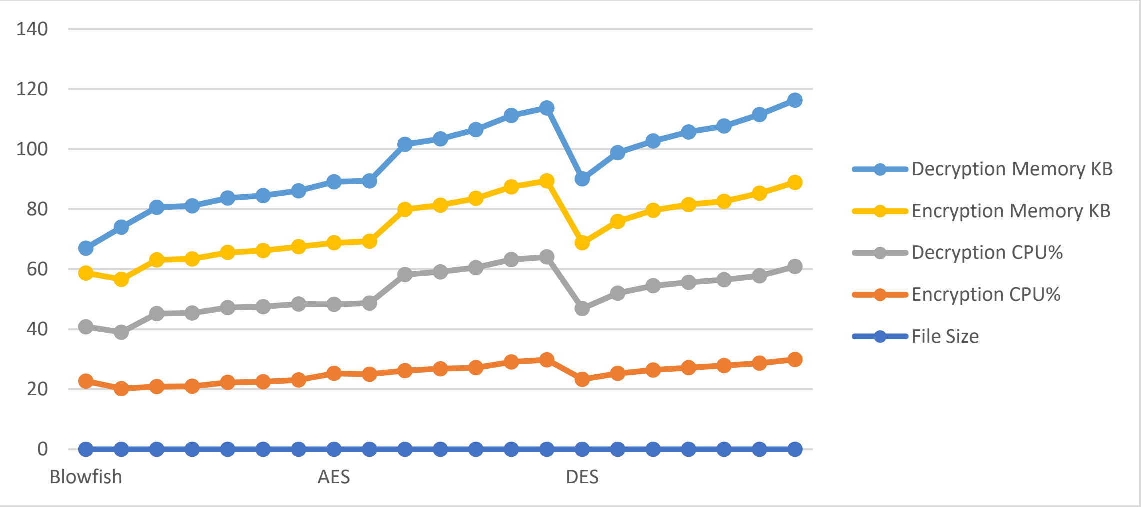

Figure1.4 CPU and Memory Comparison

III. PERFOMANCE EVALUATION METRICS

Central processing time calculation with number of instructions in program and average cycles per instruction with clock time were calculated for PEM.

Central processing time is calculated at number of instructions in program with average cycle per instruction with clock cycle time.

CPU=Inst* CPI*CT

Where CPU-CPV Time

Inst-number of instructions in program

CPI- Cycle per instruction

CT- Clock cycle Time

Performance calculation of a program is calculated as Instruction or a program X clocks or an Instruction X seconds or a clock gives a program performance calculation. Memory calculation is,

TM-(F+B+C) =Current total memory usage.

Where TM-Total memory, F- Free, B- Buffer, C- Cached.

IV. CONCLUSION

It is mainly based on the parameter results like encryption time, decryption time and also the central processing unit time with memory where an algorithm has a high confidentiality, security and integrity of data that is stored in the cloud. Security is analyzed based on the resource available by AES, DES, and blowfish. In future, encryption techniques take less time with minimum energy consumption.

REFERENCES

1. M.Q. Zhou, R. Zhang N. Xie, W.N. Quian and A. Zhou, “Security and privacy in cloud computing: A Survey,”2010 sixth international conference on semantics knowledge and grids (SKP), PP.105-112, DOI-1-3 NOV 2010.
2. GunpreetKaur and Manish Mahajan (2013), Analyzing Data security for Cloud Computing using Cryptography Algorithms, International Journal of Engineering Research and Applications, VOL-3, 782,786.
3. H T Dinhetal, “A Survey of mobile cloud computing: Architecture, Applications and Approaches, Wireless Communication Mobile Computing,Vol.13 No. 18 PP.1587-1611, 2013.
4. DuttaP, Dutta R,Mukhopadhyay S,Fully Secure online /offline predicate and attribute-based encryption in:Information security practice and experience, Springer:2015. P.331-345.
5. DWang and P Wang,” On the usability of two factor Authentication,” inproc 10thInternational Conference Security Privacy Communication Network, September 24-26,2014, PP. 141-150.
6. M Sujithra and G Padmavathi, “Ensuring Security on Mobile Device Data with two phase RSA algorithms over the cloud storage”, Journal of Theoretical and Applied Information Technology, VOL. 80, No.2, ISSN :1992-8645, October 2015.
7. W A Jansen, “Cloud Computing hooks: Security and Privacy issues in Cloud Computing proceedings of the 44th Hawaii International Conference on System Sciences, 2011.
8. J. Heiser and M. Nicolett, “Assessing the security risks of cloud computing,” Gartner Report, 2009. [Online]. Available: http://www.gartner.com/DisplayDocument? id=685308.
9. M. Jensen, N. Gruschka, and R. Herkenhoner, “A ¨ survey of attacks on web services,” Computer Science - Research and Development (CSRD), Springer Berlin/Heidelberg, 2009.
10. S. Gajek, T. Jager, M. Manulis, and J. Schwenk, “A Browser-based Kerberos Authentication Scheme,” in Computer Security - ESORICS 2008, 13th European Symposium on Research in Computer Security, Malaga, ´ Spain, LNCS 5283. Springer, 2008, pp. 115–129.

AUTHORS’ PROFILE

Harihara Krishnan R is currently pursuing Ph.D. at Presidency College (Autonomous), Chennai in the Department of Computer Science. His areas of interest are Cryptography, Computational linguistics and Computer Simulation. He is also very much interested in the field of Sign language. Paper presentations in various international conferences have made him a well-known person in the area of cryptography. He did his M.Sc. Computer Science at Loyola College (Autonomous), Chennai and was the gold medal winner of the year.

Aby John is currently pursuing Ph.D. at Presidency College (Autonomous), Chennai in the Post Graduate and Research Department of English. He has published several research papers in reputed international and national journals. Altogether he has published 13 research articles in peer reviewed national and international journals. Recently, he published two research papers as chapters in two edited books with ISBN. His areas of interest are ELT, cross-cultural business communication, applied sociolinguistics, computational linguistics and postcolonial studies. Several international as well as national conferences have boosted his profile to a great extent.

He is also a great contributor in the realm of language studies, human rights and sociolinguistics.

Dr. Amali Asha is working at Loyola College, Chennai, in the Department of Computer Science. She has published more than 15 papers in reputed International Journals. She has authored two books. She has completed one UGC-SERO funded project for the visually challenged students. Her areas of interest are artificial intelligence, swarm intelligence and image processing.

Venisha Leena Mary R has 23 years of teaching experience in various levels and is currently pursuing Ph.D at Periyar University, Salem, Tamil Nadu. Her areas of interest are cloud computing, cryptography and data structures. She has presented research papers in various international and national conferences.