International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217620

Data Storage Security in Mobile Cloud Computing (MCC) using Improved Blowfish Algorithm

Seada Abdu Wakene[1], Sisay Muleta Hababa[2], Gutema Seboka Daba[3], K S Ananda Kumar[4*]
School of Computing & Informatics, College of Engineering & Technology, Dilla University, Dilla, Ethiopia

Article Info
Volume 7, Issue 6
Page Number: 100-111

Publication Issue :
November-December-2021

Article History
Accepted : 10 Nov 2021
Published : 20 Nov 2021

ABSTRACT

Mobile cloud computing (MCC) combines cloud computing and mobile computing to deliver vast computational resources to mobile consumers, network operators, and cloud computing providers. You may access your data from anywhere in the globe using any mobile device that is linked to the Internet. Cloud computing provides access to data in real-time whenever and wherever want. Any conventional mobile device can benefit from MCC's infrastructure, computational capacity, software, and platform services. Network security, web application security, data access, authentication, authorization, data confidentiality, and data breach are all concerns of MCC's security. Because mobile devices lack sufficient storage and processing power, their data storage capacity is limited. Users of mobile devices may inadvertently provide sensitive information over the network or through the application. Therefore, data security is the main concern for mobile device users. The objective of this paper is to find a solution that can enhance technical requirements with relation to user's data security and privacy in mobile cloud computing. To achieve this improved blowfish encryption algorithm is used to encrypt each user's data security and where the shared secret key is hash down using message digest called secured hash function. Hashing can increase the integrity and privacy of user data. The proposed algorithm is evaluated with a normal blowfish algorithm and 3DES with different parameters. Improved blowfish algorithm shows better performance than normal blowfish algorithm and 3DES. In this work, we have developed web-based application where the Amazon MySQL RDS database is used for data storage.

Keywords : Blowfish algorithm, Cloud computing, Mobile cloud computing (MCC), Secured hash function.

I. INTRODUCTION

Handheld gadgets such as smartphones, tablets, and laptops have become a vital part of human existence in today's world since they are incredibly convenient and effective communication tools at any location and at any time [1]. A new technology called mobile cloud

computing has arisen to overcome the constraints of handheld devices. It mixes cloud computing and mobile computing. The concept of mobile was presented not long after cloud computing was launched in mid-2007 [2]. Mobile cloud computing has attracted the attention of a large number of industrialists because it lowers the cost of developing and running mobile applications. With modern smart phones and powerful mobile devices, mobile apps provide many advantages to the community but it has also grown the demand for online availability and accessibility. Cloud computing is provided to be widely adopted for several applications in mobile devices [3].

Data replication, consistency, restricted scalability, instability, unpredictable availability of cloud resources, portability (due to a lack of cloud provider standard), trust, security, and privacy are all issues in the field of mobile cloud computing [4].

Dr. U S Pandey's 2018 research report is the first thing that motivates us. It shows that data security and privacy, user authentication and authorization, and user access in mobile cloud computing are all hot topics in research these days. This is because once data leaves the protected environment of mobile devices; it is exposed to a variety of harmful threats both on the device and in the cloud.

The second thing that motivates us to undertake this work is the fact that mobile cloud computing advantageous computing choice for businesses, organizations, institutions etc. Still the security challenges for this technology are not addressed adequately. Because of this reason, we chosen this research work and make contribution to this research area.

The rise of mobile cloud computing has not been accompanied by an increase in consumer trust in cloud-based data management in various industries. Because of the hazards of confidentiality and privacy, several businesses are hesitant to utilize cloud computing mobile services [5]. Therefore, data security is the main issue that should addressed. Confidentiality and massage integrity among them requires high guaranteed security. MCC inherits all of the security challenges associated with cloud computing, as well as the resource constraints imposed by mobile devices. Due to resource limits, the security methods proposed for the mobile cloud-computing environment cannot be directly run on a mobile device. A lightweight secure framework that delivers security with the least amount of communication and processing overhead is required for mobile devices [6].

There are different security algorithms are used to encrypt data store. These are asymmetric and symmetric. Asymmetric encryption techniques are slower than symmetric encryption techniques because they require more computational processing capacity [7]. Therefore, we prefer to use symmetric algorithm since mobile device have low processing unit and storage space. There are different security algorithms are DES, AES, 3DES, Blowfish Algorithm.

In this work, we select symmetric algorithms, which have high performance, high speed, and which keep data confidentiality and privacy. Therefore, we choose blowfish algorithm, which is fastest symmetric encryption algorithm.

The main objective of this work is to secure data stored on cloud by mobile device using symmetric cryptographic algorithm called Improved blowfish algorithm.

II. LITERATURE REVIEW

Cloud computing is a term used in computer networking to describe many computing ideas that involve a large number of machines connected by real-time communication, such as the internet [8], [9], [10]. Cloud computing is also known as distributed computing via the network, which refers to the

capacity to run a program or application on multiple computers at the same time.

They define mobile cloud computing and present a summary of the findings from this review, focusing on models of mobile cloud applications, in [11]. They also point out some of the research problems in the field of mobile cloud computing. They end with suggestions on how a deeper grasp of mobile cloud computing might aid in the development of more powerful mobile apps. Mobile cloud computing is a novel computing paradigm in which processor, memory, and storage resources are not physically present at the user's location. Instead, these resources are owned and managed by a service provider, and consumers can access them via the Internet. For example, Amazon Web Services' Simple Storage Service (S3) allows users to store personal data and run computations on it using the Elastic Compute Cloud (EC2). Low initial capital investment, faster start-up time for new services, lower maintenance and operation expenses, increased utilization through virtualization, and easier disaster recovery are just a few of the benefits that make cloud computing an appealing alternative. According to reports, there are also a number of security issues, which are explained as an open research topic.

This study [12] provides an in-depth look of mobile cloud computing, covering definitions, architecture, and rationale for development, benefits, problems, and future research possibilities. Cloud computing is described for a better understanding of mobile cloud computing before it is described. MCC, as defined by the authors, is an infrastructure in which both data storage and data processing take place outside of the mobile device. They define as integration of mobile web and cloud computing. The paper lists the advantages of MCC are On-demand services, low cost, robustness and flexibility. They also address the challenge from the list security and privacy is the main issue that should be fixed.

The author of [13] evaluated the most recent research and advancement in secure cloud mobile computing. The first looked at three different cloud architectures that are geared to accommodate future cloud-based mobile computing models. They demonstrated that when the advantages of mobile devices and cloud computing are combined into one system, new features may be achieved to increase the computing capabilities of mobile devices. They then looked at a variety of challenges to mobile cloud computing infrastructures' availability, privacy, and integrity. In comparison to typical client-server architectures, they demonstrated that attackers could target and exploit a considerably larger range of resources/protocols in a mobile cloud-computing environment. Finally, summarized recently proposed defence techniques for securing mobile cloud computing systems and applications. The limitation is only preparing secure architecture not securing stored file, and mobile devices. It has the limitation of time of retrieving data.

Mobile user authentication strategy for mobile cloud computing in this paper [14], which is based solely on cryptographic hash, bitwise XOR, and fuzzy extractor functions. They produced a formal security proof using the XOR model, as well as a formal security verification using the ProVerif 1.93 simulation program. Furthermore, the BAN logic provides reciprocal authentication evidence. The suggested technique has a low calculation cost when compared to existing relevant schemes because it does not use any resource limited cryptosystems. Because the proposed technique does not use RC in the authentication process, it has a lower communication cost than similar schemes already in use. Overall, the suggested approach is well suited for practical implementations in the mobile cloud computing area because to its excellent security and cheap communication and processing costs. The limitation on this paper discuss in authentication rather it does not data confidentiality, integrity and availability.

Different security mechanisms used in mobile cloud computing and their efficiency were addressed in [15]. The security and privacy of data kept in Cloud Computing is a complex issue with critical

implications. To guarantee safe connection between the user and the cloud, cryptographic techniques were used. To guarantee safe connection between the user and the cloud, cryptographic techniques were used. It examines the differences between symmetric and asymmetric algorithms. Showed that symmetric encryption has the speed and computational efficiency to handle encryption of massive volumes of data in cloud storage, and that DES is a better encryption algorithm. However, DES takes longer to encrypt data and has a lower throughput than other symmetric encryption algorithms.

The Internet and network applications are rapidly expanding. As a result, the importance and value of data shared over the internet is growing. In data communication, information security has always been a major concern. Any loss or threat to information can result in a significant financial loss for the company. In information security systems, encryption plays a critical function. This study compares and contrasts four of the most widely used symmetric key algorithms: DES, 3DES, AES, and Blowfish. The following factors were used to make a comparison: round block size, key size, encryption/decryption time, CPU process time in terms of throughput, and power consumption. These findings suggest that blowfish is a better option than AES [16].

In terms of encryption time, decryption time, and throughput in wireless networks, this paper [7] provided a fair comparison of AES, DES, 3DES, and Blowfish. According to the simulations, Blowfish performs better in terms of encryption time, decryption time, and throughput. The second aspect to note is that, with the exception of Blowfish, AES has an advantage over the other 3DES and DES in terms of throughput and decryption time. At the third point, 3DES has the worst performance in terms of decryption process throughput under the identical conditions.

The three papers [11], [12] and 13] cover the overall meanings of mobile cloud computing. They explain about advantages and disadvantages. They give security issue is the main open research area that should be fixed. The papers [15] and 16] give solution to overcome but there is also limitation on that paper that is open for the researcher to be addressed. The observed algorithms are time consuming and have low throughput. The paper [7] and [14] address best algorithm that have high performance and which increase confidentiality as well as integrity in cryptography in wireless network. Bhavyashree et.al proposed a IBDO scheme provides strong security by using efficient algorithms. It quickly finds out unauthorized person who tries to make modification on storage files. It also finds misuse of authorization [17].

The limitation observed on the related work will be addressed by this research work through the implementation of mobile cloud web-based application that uses improved blowfish algorithm to encrypt file upload on the cloud and where the randomly generated secret key is, send to the client user to decrypt and see their file.

Kandavel et. al proposed for a mobile data security and end-to-end mobile cloud connection, the Royal Seal Cloudlet (NRSC) is a revolutionary Royal Seal Cloudlet (NRSC). The suggested NRSC approach is based on the use of a unique random private token for each trusted user. It's a group of mobile guests who work together to deliver a better security service or execution environment [18].

Karthikeyan et.al proposed a algorithm, wrapped thread is combined with the hash value created by the SHA-256 technique to secure the transmission, and the secret key is exchanged via the DiffieHellman algorithm. A unique offloading algorithm is proposed to improve energy efficiency [19]. In [20] proposed a research project presents a secure cloud computing mobile environment that provides users with valuable services. The proposed methodology has a 98.5% success rate in providing secure communication services to consumers via cloud computing apps, according to experimental results.

The goal of the research work explained in [21] is to show how to ensure mobile data storage privacy and secrecy in a cloud communication environment using mobile training datasets and the Training dataset Filtration Key Nearest Neighbor (TsF-KNN) classifier, which classifies data depending on its level of confidentiality.

III.METHODOLOGY

Proposed System

The proposed model uses, Improved Blowfish algorithm in MCC. The proposed system is a cloud web-based application, which is developed by a symmetric cryptographic algorithm called blowfish algorithm. This system allows the cloud service user to manage and upload data into a cloud-computing environment. The application is developed on a local machine and on an Amazon RDS MySQL database engine where the database is developing and run on the cloud.

The figure 1 explains the workflow of the system. The admin uploads a file on the cloud and the data is encrypted using blowfish algorithm before it is stored on the database and at the same time, secret key is generated for the decryption process. Before decrypt, the cipher text the user requires the secret key and id of the file, (one time) which is generated from the server to the client. The secret key is send to the client through their email address during access request after the client LOGIN in to web through their email address and password. Then the encrypted file will be decrypted using the secret key and the client can gain the plaintext (their original file). If the one-time key and id of the file is not same out of time and incorrect massage will be generate.

The figure 1 shows the general work flow of data security in mobile cloud computing which contains encryption and decryption process.

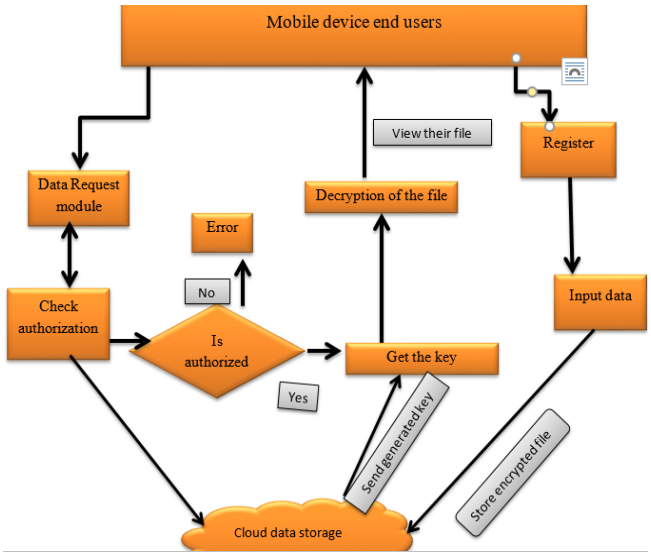

Figure 1 General work flows with different module for the data security

A. Step wise procedure to develop

It is involving on development of cloud-based application to ensure the cloud data security using blowfish algorithm.

- Selecting secured encryption algorithm on cloud
- Developing web based application on cloud and can provide can be secure user data using java servlet and java servlet package

Blowfish algorithm used and implemented by java security package.

B. Architecture of the system

The proposed architecture explains the general workflow. The external users are clients that are register to access manage and store their data on the web service and they can access and communicate through web browser. The web browser connects with the application server and used to develop web app and server environment to run on it. It can also help for effective execution of program, scheduling, and scripting. This will execute the blowfish algorithm encryption algorithm needed to secure the user's data. The database used to store file and retrieve a file that is move through the application sever when client need their data. The database is required to

extract the data and display on the website via the application server.

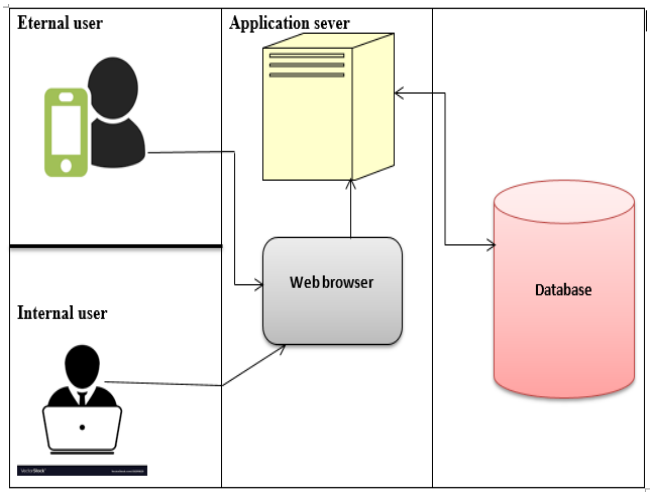

Figure 2 Architecture of the system

C. *Steps to develop the system*

An organization can use both private and public cloud in order to store bulky employee and customer data records and other management system information. For any record system, we have used the following step to store and retrieve their information. The admin accept any file from the mobile client that is authenticated and encrypt the file using improved blowfish algorithm and store in the cloud. The clients decrypt their file using the key generated by sever and file id then view their file. There are three steps for proposed system they are explained below.

Our proposed method is followed by three steps

❖ *User Registration*

1. Admin register new users
2. Server upload user's data (Name, Email, Phone, Password (encrypted)
3. Send email to the user with login information

❖ *File retrieving*

1. User receive id of the file with its secret key
2. Provide id and key to the server
3. Server retrieves the file using its id
4. Decrypt the file with the provided secret key and download the file

❖ *File uploading*

1. Admin upload file to the server
2. The server generates random key or one-time key.
3. The server encrypts the file and store encrypted file to specific location and required data to the database (name of the file, type of the file (encrypted), and secret key of the file (encrypted)
4. Send email for users with file Id and secret key of the file

D. *Improved Blowfish algorithm*

For our proposed system, we prefer to use blowfish algorithm, which is categorized under symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Since it uses same key it need more protection from hackers and attackers. Therefore, we prefer to encrypt the generated key using massage digest, which call secured hash function. Using massage digest can increase integrity. The key generated is hash down to 160 bit by using massage digest and prepare long bit encryptor. Then p-box and s-box is initialized the process is gone until get the encryptor. After getting encryptor, the encryption process is starts. When encryptor is gain, automatically random long independent variable is generated that is unique for every cipher text. A decryption process is the same as encryption process only reverse order. Below the three processes, give encryption decryption process using proposed algorithm.

Process 1: Setup Encryptor using secret key

Step 1. Get secret key
Step 2. Hash down the key to 160 bit key by using Message digests and returns byte data key.
Step 3. Initialize p-box and s-box
Step 4. XOR the byte key over the p-box
Step 5. Encrypt p-box and s-box with all zero string
Step 6. Return Encryptor

Process 2: Encryption

Step 1. Generate random independent value(IV)

Step 2. Allocate byte with size of original data plus 8 byte padding

Step 3. Copy all bytes of the original data in to a buffer of type byte

Step 4. Get Encryptor generated in the above process while generating secret key

Step 5. Loop through the buffer by incrementing by 8

a. Encrypt 64 bit block by

i. Converting to long

ii. Chain the block with the independent value(IV)

iii. Break the block into two 32bit blocks and perform the default blowfish algorithm swap and XOR process

iv. Return encrypted block

b. Change the independent value(IV) equal to the new block and return the value

c. Change log to byte array

Step 6. Combing the buffer byte data

Step 7. Return binhex cipher data by converting the byte to binhex.

Process 3: Decryption

Step 1. Get the number of estimated bytes in the binhex cipher text

Step 2. Make sure size of the text is equal to block size

Step 3. Get the independent value(IV) from the cipher by converting the binhex to bytes

Step 4. After getting the independent value (IV) and bytes buffer do the same as Encryption but the p-box value in reverse order.

Step 5. Return the string by converting the byte array to UNICODE string Model of the proposed system is to encrypt any file accepted from the client using blowfish algorithm. Then the file converts in to cipher coded file this cipher coded file. This cipher coded file is decrypted using the hashed secret key to get the original file.

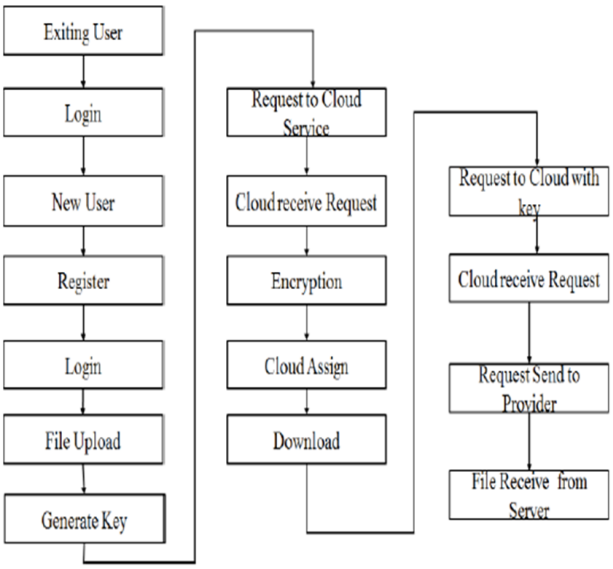

Figure 3 Overall flow of the proposed system

IV. RESULTS AND DISCUSSION

A. *Performance analysis*

Experiments for performance evaluation are carried out in this section. On the Java platform, the proposed technique is implemented. The encryption and decryption times, as well as the throughput are calculated. All of these technologies not only secure data, but also control access to encrypted data on a cloud network while comparing the data.

The suggested system uses an updated blowfish algorithm to encrypt and decrypt various input files of varying sizes (in kb). This technique was created for security reasons, as well as to reduce "encryption and decryption procedure" execution times. The upgraded blowfish encryption approach's security is put to the test.

B. *Performance metrics*

Encryption time (milliseconds), decryption time (milliseconds), and throughput are the performance measures. The following are the performance metrics that have been examined and discussed:

Encryption Time: It is the amount of time it takes for an encryption algorithm to generate a cipher text from plain text. The throughput of an encryption process is calculated using encryption time. In other words, it shows the encryption process's speed. In most cases, the encryption time is measured in milliseconds. It is the amount of time it takes an encryption algorithm to encrypt data. The shorter the encryption time, the better the algorithm's performance.

Decryption Time: It is the time it takes an encryption algorithm to convert a cipher text to plain text. The throughput of a decryption process is calculated using decryption time. In other words, it indicates how quickly the decryption process is completed. Decryption times are usually measured in milliseconds. It is the amount of time it takes an encryption technique to decrypt data. The shorter the decryption time, the better the algorithm's performance.

Throughput: The ratio of total plain text to encryption or decryption time is used to calculate the encryption scheme's throughput [3]. The higher the throughput value, the more efficient an encryption method is at encrypting any content.

Throughput of Encryption Algorithm = Tp (Kbytes) / Et (Milliseconds)

Where;

Tp: Total Plain Text (Kbytes) Et: Encryption Time (Milliseconds)

Encryption Time: shows the encryption time of 3DES, Normal Blowfish and Improved Blowfish on different file sizes.

Decryption Time: shows the decryption time of 3DES, Normal Blowfish and Improved Blowfish on different file sizes.

Throughtput: shows throughput of 3DES, Normal Blowfish and Improved Blowfish on different file sizes.

Key Generation Time: Shows the key generation time of symmetric. Key generation time is depending on the bit length of a key. Performance of encryption algorithms, 3DES, Normal Blowfish and Improved Blowfish are evaluated considering the following parameters

- Key size in bits.
- The time consumption signature generation and verification.

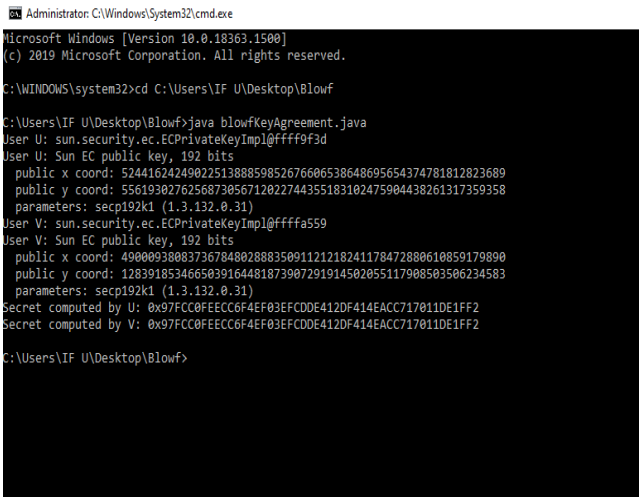

Figure 4 Sample key generation

C. *Results and Analysis*

In this research work, developed a prototype of data security for mobile cloud computing using improved blowfish cryptographic encryption algorithm. The mobile device users are able to store file without any fear any attacker. Since the proposed system can give privacy, confidentiality secure for any users that store their file on cloud.

The table 1 give the sample file stored in the database that is encrypted and stored and the secret key that is hashed and store on the cloud that generated by the sever during file uploaded.

TABLE 1 : ENCRYPTED FILE AND SECRET KEY STORED

File	Secret key
df24411e0874d74a2f1 bfba6d460372d8cdd0 dbd4a37ae	104358d0cd48fd720d9bc 374ba7ecc515e65a6c654 62a253f9…
0e3e16b2b0beaf61a52 3ff725eb5ac066a4996	325f31237056ba35b3b6b 13ba26c723144b2013574

885be38486	24dd750f…
41c78b9d63258761e3a50896c33f4f4624c35cabc86ddc4db5	857853c12c9308586b35fbb91f138e43c7a232143132bdc88f…

Figure 5 shows sample emails send the secret key and file id used by mobile user to decrypt their file. By copying the file id and decryption key user can get their original file.

Figure 5 Sample email sent secret key and file id

D. Analysis of Overall comparison of algorithms

TABLE 2 ENCRYPTION AND DECRYPTION TIME WITH FILE SIZE OF THE ALGORITHM

Algorithm	File size(Kb)	Encryption Time (milli sec)	Decryption Time (milli sec)
DES	16	8.4375	13.75
Normal Blowfish Algorithm	32	6.4341	5.1587
Improved Blowfish	64	5.95	4.3

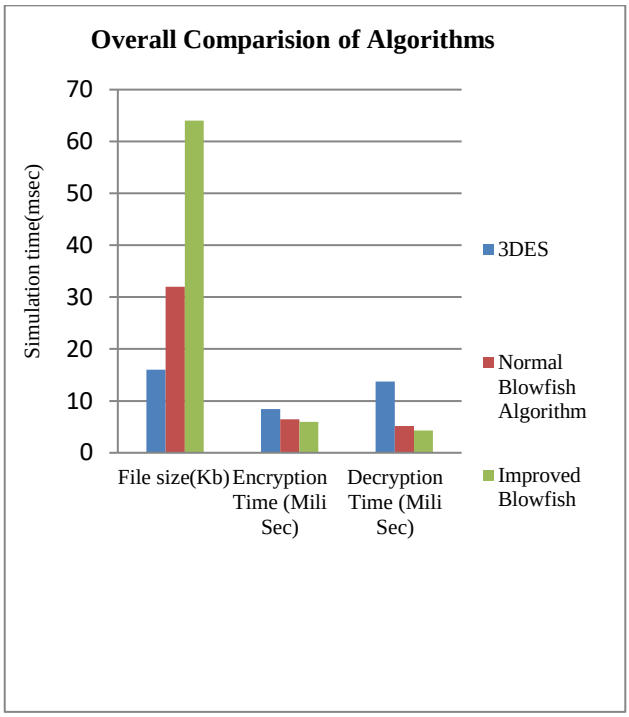

Figure 6 Overall comparisons of algorithms

Simulation results for this comparison point are shown fig 6 and table 2 encryption and decryption times with different bit key length and with different size data block. We can find in decryption and encryption time of the improved blowfish has the less than normal blowfish and 3DES algorithms that mean improved blowfish algorithm is fast encryption algorithm.

TABLE 3 BLOCK OF SIZE WITH TIME CONSUMING OF ALGORITHM

Algorithms	Data block size in kb	Time in msec
3DES	2	1.78
Normal Blowfish	4	1.67
Improved Blowfish	6	1

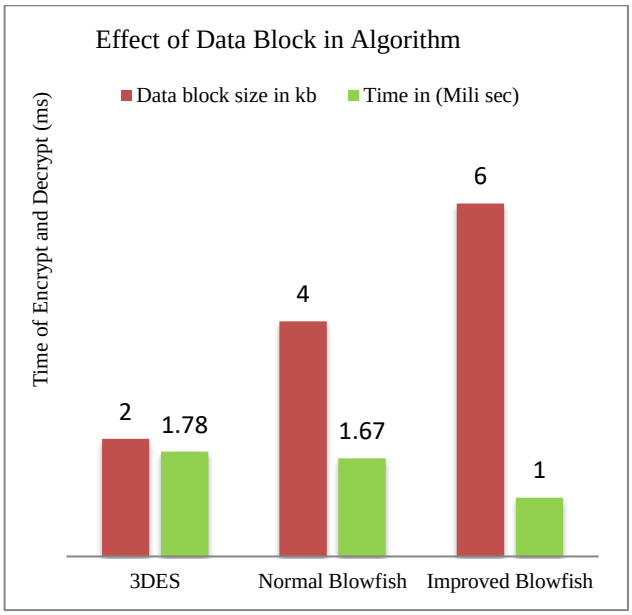

Figure 7 Effect of data Block in Algorithms

Simulation results for this comparison point are shown in figure 7 and table 3 encryption time and decryption time with different size data block. We found that blowfish and 3DES algorithms have high encryption time and decryption time as compared to improved blowfish algorithm.

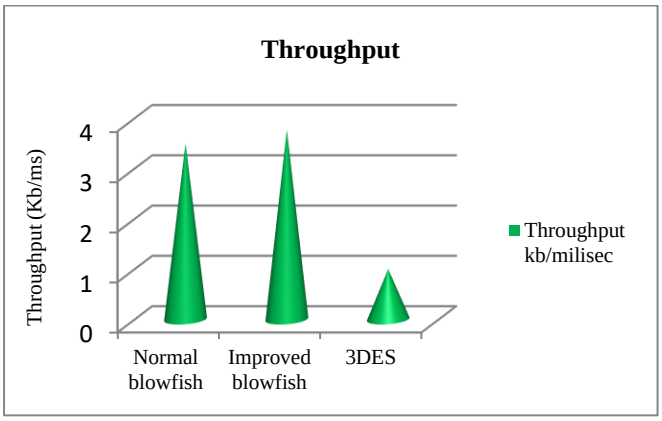

Figure 8 Throughputs of Algorithms

The figure 8 comparison indicates that normal blowfish and 3DES algorithms shows low throughput as compared to improved blowfish algorithm.

The improved blowfish algorithm is compared with 3DES and normal blowfish algorithm with encryption time, decryption time and throughput. The result shows that normal blowfish algorithm is better than DES but less than the improve blowfish algorithm.

V. CONCLUSION

Mobile cloud computing is one of the fastest-growing cloud computing environments in worldwide which able to access anywhere, any time by the mobile device user. Even though it has a huge advantage, it has also security threats that should be addressed. Data security has a great role from the security issue raised on mobile cloud computing since most the client data store on the cloud.

In this research work, proposed a solution that allows data to be secured by implement improved blowfish cryptographic encryption algorithm to encrypt any file upload by mobile device user and store on the cloud. Using improved blowfish with encrypted key can increase the security able to fulfil the all security principles such as privacy, confidentiality, integrity. Our proposed work only allows the authorized user can access their data. An attacker cannot decrypt the data until it gets the encrypted secret key and file id that is generated by the cloud server. In terms of encryption time, decryption time, and throughput, we gave a fair comparison between enhanced blowfish, 3DES, and Blowfish. In comparison to 3DES and the normal blowfish algorithm, the simulations indicated that Improved Blowfish had greater performance in terms of encryption time, decryption time, and throughput.

VI. FUTURE WORK

Comparison of different symmetric algorithm with improved blowfish algorithm with different parameters in mobile cloud computing environment. Evaluating different asymmetric algorithms with the improved blowfish algorithm.

VII. ACKNOWLEDGEMENTS

The authors would like to express sincere thanks for the encouragement and constant support provided by the School of Computing & Informatics, COET, Dilla University, Dilla, Ethiopia during this work.

VIII. REFERENCES

[1]. M. Computing, M. Padma, and M. L. Neelima, "Mobile Cloud Computing : Issues from a Security Perspective," vol. 3, no. 5, pp. 972–977, 2014.

[2]. A. Oludele and O. Oluwabukola, "A survey of mobile cloud computing applications: Perspectives and challenges," 7th Int. Multi-Conference Complexity, Informatics Cybern. IMCIC 2016 7th Int. Conf. Soc. Inf. Technol. ICSIT 2016 – Proc., vol. 1, pp. 238–243, 2016.

[3]. R. Kaur and S. Kinger, "Analysis of Security Algorithms in Cloud Computing," vol. 3, no. 3, pp. 171–176, 2014.

[4]. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[5]. S. Subashini and V. Kavitha, "Journal of Network and Computer Applications A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., 2010.

[6]. A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Futur. Gener. Comput. Syst., vol. 29, no. 5, pp. 1278–1299, 2013.

[7]. G. Singh, A. Kr. Singla, and K. S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks," Int. J. Comput. Appl., vol. 44, no. 11, pp. 23–26, 2012.

[8]. N. Jose and C. K. A, "Data Security Model Enhancement In Cloud Environment," vol. 10, no. 2, pp. 1–6, 2013.

[9]. R. G. Saranya and A. Kousalya, "A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing," vol. 8, no. 2, pp. 306–310, 2017.

[10]. P. Mell and T. Grance, "The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology," Public Cloud Comput. Secur. Priv. Guidel., pp. 97–101, 2012.

[11]. R. A. Bajad, M. Srivastava, and A. Sinha, "S m c c," vol. 1, no. 2, pp. 8–19, 2012.

[12]. M. R. Momeni, "A Survey of Mobile Cloud Computing : Advantages , Challenges and Approaches," vol. 15, no. 4, pp. 14–28

[13]. Gu, Qijun, and Mina Guirguis. "Secure mobile cloud computing and security issues." In High Performance Cloud Auditing and Applications, pp. 65-90. Springer, New York, NY, 2014.

[14]. S. Roy, S. Chatterjee, and A. K. Das, "On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services," vol. 5, 2017.

[15]. T. Chithambaram and M. Durairaj, "Networks Security on Mobile Computing – A Survey," vol. 6, no. 04, pp. 168–174, 2015.

[16]. P. C. Mandal, "Evaluation of performance of the Symmetric Key Algorithms : DES , 3DES , AES and Blowfish," J. Glob. Res. Comput. Sci., vol. 3, no. 8, pp. 67–70, 2012.

[17]. Bhavya Shree M N, K S Ananda Kumar, Kavyashree S, Gagana H, S Geetha; Accessing Data In Cloud Platform Using Identity And Providing Strong Security, Auditing Based On IBDO Scheme; Global Journal of Engineering Science and Researches [ICRTCET-2018]; 2018, pp 54-61.

[18]. Kandavel, N., and A. Kumaravel. "A Novel Royal Seal Cloudlet for Security Enhancement in Mobile Cloud Computing." International Journal of Computer Science and Information Security (IJCSIS) 17, no. 1 (2019).

[19]. Karthikeyan, B., T. Sasikala, and S. Baghavathi Priya. "Key exchange techniques based on secured energy efficiency in mobile cloud computing." Applied Mathematics & Information Sciences 13, no. 6 (2019): 1039-1045.

[20]. Sridhar, S., Smys, S. Hybrid RSAECC Based Secure Communication in Mobile Cloud Environment. Wireless Pers Commun 111, 429–442 (2020). ttps://doi.org/10.1007/s11277-019-06867-0

[21]. A. Inani, C. Verma and S. Jain, "A Machine Learning Algorithm TsF K-NN Based on Automated Data Classification for Securing Mobile Cloud Computing Model," 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019, pp. 9-13, doi: 10.1109/CCOMS.2019.8821756.

Cite this article as :

Seada Abdu Wakene, Sisay Muleta Hababa, Gutema Seboka Daba, K S Ananda Kumar, "Data Storage Security in Mobile Cloud Computing (MCC) using Improved Blowfish Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 100-111, November-December 2021. Available at doi : https://doi.org/10.32628/CSEIT217620
Journal URL : https://ijsrcseit.com/CSEIT217620