Hybrid Security System for Mobile Cloud Computing

[1] Abdulsalam Shettima Nur and [2] Abubakar Muhammad Miyim

[1]Department of Computer Science
Federal University Dutse

[2]Department of Information Technology
Federal University Dutse

Corresponding Author: abdulsalamshettima@gmail.com

Abstract
The rapid growth of mobile cloud computing, information sharing and communication have become easier due to convenience, wide reach, relatively low cost, and ability to support the achievement of real-time interaction. The Mobile cloud computing makes it easy for humans to access data and as time goes by, a large storage capacity of data is needed to maintain such data in terms of security. This development therefore calls for a better data security system to secure data from various threats such as data integrity, data confidentiality and data access. This research has been undertaken to enhance the data security of mobile cloud computing using hybrid algorithm. The Proposed method consists of two algorithms, Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA). The proposed method was implemented using Python programming language, and the performance in terms of time complexity of encryption and decryption was measured, data integrity and confidentiality was verified and compare against existing methods. The results show that the proposed method has the best-case time efficiency in encrypting and decrypting data, it is also more reliable and secure than the existing methods.

Keywords: Mobile cloud computing, encryption, decryption, data integrity & confidentiality.

INTRODUCTION

With the rapid advancement of mobile devices, people can easily access information, exchange messages and much more. As a result, the number of people using mobile device is growing every day, because the mobile devices have become an almost inseparable part of everyone's life. Two-thirds of humanity owns a mobile device [2] and more than 50% of the world's population is now online; roughly one million more people join the internet each day [1]. To this end, advanced mobile technologies have given rise to the rapid growth of mobile cloud computing [3].

Mobile devices face a lot of challenges such as battery life, storage capacity, bandwidth e.t.c. and the limited resources has significantly affected the quality of services offered by mobile computing (MC). While cloud

computing (CC) offers unlimited advantages to users by allowing them to use infrastructure, platforms and software by cloud providers at low cost and elastically in an on-demand fashion [4].

The mobile cloud computing (MCC) aim to overcome the limitations of Mobile computing and cloud computing by integrating into single environment to bring new type of services and facilities for mobile users [5]. MCC refers to an infrastructure where both the data storage and data processing happen outside the mobile device. Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds which are then accessed over the wireless connection based on demand fashion [6].

The MCC has been identified as the next generations computing infrastructure and the worldwide cloud computing market continues to grow and is expected to reach an estimated 482 billion U.S dollars in 2022 [7].

Nowadays, MCC are becoming an integral part of society in various domains and discipline these include education, health, finance, business, transportation, social media, and many more. For example, today almost all educational institute are using this technology to keep students results and records. Furthermore, this technology is continues growing rapidly among the users due to information availability at their fingertips anywhere anytime, so that users can access data in mobile cloud computing environment through mobile devices. It also provides an optimal service for mobile users in terms of storage capacity, cost effective, flexible, reliable, maintainable and may more but there are security challenges which are important and necessary to address the issues such as data integrity, data confidentially, data access, etc.

Security breaches in mobile cloud computing system.

There is no doubt that the growth of mobile technology poses a threat to the society and the growing reliance on computing systems, networks and has equally witness an unprecedented rise in cybercrime which becomes a worldwide problem immune to all countries. In recent years, more organizations have become increasingly dependent on cloud systems for their day-to-day operations. On the other hand, there is an increase in the number of security breaches affecting several organizations and individuals, newer attacks are resurfacing which require serious attention of security experts. According to [8] companies suffer from cyberattack at least once a year. Because of those high risks of security breaches in the computing world, the business sector must also consider the network security mechanism as a commodity input [9].

In the world of computing, information is power; it's an asset that has to be protected against attackers. These days, the invention of newer mobile devices and cloud computing

technologies increases the rate of cyber-attacks across the globe. Hackers are now taking advantage of weak security implementation to control remote networks using malicious code, vulnerability tools, and other programs to attack targets to violate data integrity, privacy and steal or damage remote data.

However, even though there are a large number of benefits of mobile cloud computing, but yet there are a number of security issues that were not addressed includes data integrity, data confidentiality, data access, authentication, authorization, network security, web application security etc. This raises the demand for a better data security system to secure data from those threats [10] and is one of the key areas that the cloud providers and other stakeholders are given more attention to safeguard and minimize those threats [11].

Secure data communication is of a key concern in today's computing world and various algorithm mechanisms are developed in order to achieve the data security systems but there are some complexities in the existing systems such as easy to alter, time consuming in encrypting large amounts of data and slow in generating key [12]. However, to implement an effective and efficient system, all these aspects have to be considered in order to make it robust. There is need to implement the technique which helps to overcomes such complexities in such existing systems.

RELATED WORKS

The researchers in [13] presented performance evaluation of hybrid cryptography algorithm to secure sharing of text & images. The algorithm focuses primarily on blending together asymmetric and symmetric cryptography which enhances the security level when compared with existing method that uses only asymmetric algorithm. However, one of the weakness of these paper is that the image encryption and decryption time is not efficient as it takes longer time to encrypt and decrypt image file.

In [14] a comparison of image encryption & decryption with text using AES Algorithm was adopted. The AES algorithm uses 128-bit key for encryption that makes AES secured and faster than DES, due to large key size that helps overcome attacks such as brute force attack and man-in-the middle attack. The algorithm was implemented using Java programming language to compare the efficiency of AES while considering image and text to analyse. Furthermore, the result of the work shows that the sharing of information through image is much more reliable and efficient than sharing information as a text. However, the time complexity of the text file was found to be one of the weaknesses of the paper.

The researcher [15], conducted a comparative study of hash algorithms in cryptography with detailed design of hash function such as MD5, SHA1, SHA2, SHA3 provided. Additionally, the paper focused on comparative analysis of various types of hash

algorithms but did not consider implementing any of the algorithms to address the issues.

The research work published in [16] did present an implementation of advanced encryption standard (AES) with graphical user interface using visual studio.net. Previous research works (C programming language, MATLAB, JAVA script and Visual Basic) have shown that AES was implemented using different paradigms to encipher and decipher data (text, images and videos). The paper focused on design of secured data files on computer system from unauthorized users by encrypting the data file with a specified password. The same password is however, used in decrypting the ciphered data file to obtain the actual data file. The drawback is that efficiency of the system was not measured in terms of encryption and decryption time.

In the work of [17] the researchers conducted a text encryption and decryption using AES Algorithm by proposing an algorithm that offers high encryption quality rather than other standards. There is currently no evidence that AES has any weaknesses making any attack other than exhaustive search, i.e. brute force. The researchers concluded that AES provides security to multiple accounts, multiple files which have confidential data, but no implantation of an algorithm was adopted.

[18] presented an implementation of hybrid cryptosystem with AES and SHA. The idea of the proposed hybrid cryptosystem was to use the SHA-256 bit as a key generation for AES-256 in order to improve the data security to a greater extent and also to provide higher security in terms of complexity. The hybrid cryptosystem was implemented using LabVIEW 2013 but the performance of the system in terms of encryption and decryption time was not measured and this brought the shortcoming of their work.

The research work [19] did carryout a hybrid cryptographic algorithm based on AES and SHA in Radio Frequency Identification (RFID). The RFID together with the new Internet-Of-Things (IoT) concept along has created a new realms of technology advancement by bringing lots of new innovative ideas for implementation. Consequently, data security is one of the key issues that must be considered when transmitting. The research however, presented a hybrid model to ensure security, validity and integrity assurance of the data during the transmission. Though the model was implemented with two highly strong cryptographic algorithms (SHA and AES) for encryption and decryption of the data, the performance of the model was not measured.

The Proposed Method

AES has proven itself to be secured, faster, reliable and effective method of safeguarding sensitive information over the years in cloud computing but it is hard to implement with software. While SHA produces a unique digest message for every data value which recognize it as high secured but some of the drawbacks are collision and pre image resistance.

However, the research gaps of previous researchers also show that some algorithms are slow in encrypting large amounts of data, very slow in generating key and easy to crack or alter. According to [20] the RSA algorithm has been used by different cloud providers but it has been proven to be ineffective, inefficient and time consuming in encrypting large amounts of data. In order to implement an effective and efficient system all these aspects have to be considered in order to make it robust.

Based on the research gaps we proposed a hybrid security system to enhanced the system. The proposed method is a combination of two algorithms i.e. advanced encryption standard (AES) and secure hash algorithm (SHA) that is integrated together to form a single system known as hybrid system. However, according to [21] to provide a maximum-security system, a hybrid system is required and a single system for encryption and decryption is considered to be inefficient because intrudes can easily crack or alter data but when more than one algorithm is used, it becomes more reliability and secured as it involves two major security systems and also shows the concept of Cyclic Redundancy Check i.e. data integrity is checked for both encryption & decryption which make it more reliable and safer. The proposed method is implemented using Python programming language because Python comes inbuilt with wide array of modules and libraries.

RESULTS AND ANALYSIS

After the implementation and simulation was carry out successfully, the time complexity of encryption and decryption of the proposed method was then measured and compared with the existing methods. Comparative result is shown in graphical representation in figure 1 and 2.

a) Text-file comparisons

Based on the result obtained from the existing method and the proposed method of a text file for encryption time and decryption time values are presented in table 1. Different file size was taken as input and the file sizes given in kilo byte (kb). However, the results show that the existing method take much longer time to encrypt and decrypt a text file, while the proposed method takes lesser time or few milliseconds to encrypt and decrypt each text file. Hence, the proposed method shows better efficiency and faster to encrypt and decrypt a text file than the existing method.

Table 1: Comparisons between existing method & proposed method of a text-file.

S/No	File Size (MB)	Existing methods [13] [14]		Proposed method	
		Encryption Time (ms)	Decryption Time (ms)	Encryption Time (ms)	Decryption Time (ms)
1	20	49	80	09	11
2	25	50	82	12	15
3	50	57	83	23	26
4	75	65	88	29	32
5	100	71	92	36	40
6	150	88	113	59	66
7	Average Time	63.33	89.66	28	31.66

Though, figure 1 below is the graphical representation of the results.

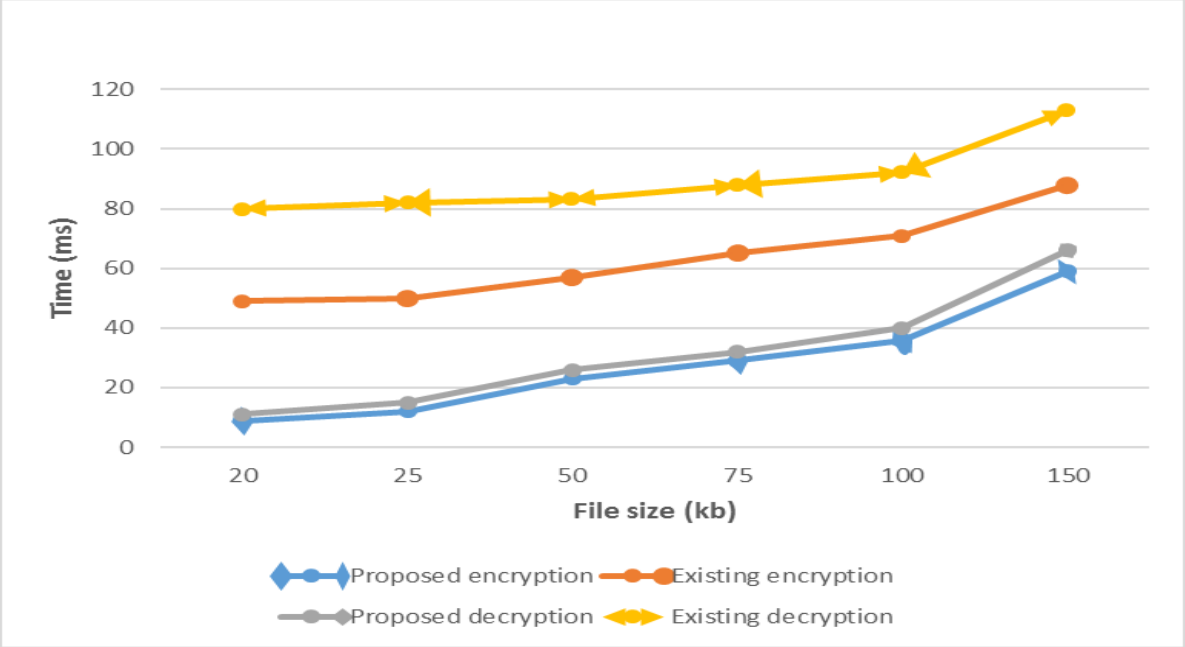

Figure 1: Graphical representation of a text-file Encryption & Decryption Time.

b) Image-file comparisons

The comparisons between proposed method and the existing methods of an image files is presented in the table 2. The same data sets were used as inputs for the comparison purpose.

Average encryption time and decryption time are computed for both the methods.

The results show that the encryption time and decryption time for the proposed method has the best-case

time efficiency, while the existing methods has the worst-case time efficiency. Hence the proposed method is more efficient in encrypting and decrypting an image file. This is shown in Table 2 below.

Table 2: image comparisons between existing & proposed method.

S/No	File Size (MB)	Existing methods [13] [14]		Proposed method	
		Encryption Time (ms)	Decryption Time (ms)	Encryption Time (ms)	Decryption Time (ms)
1	20	17	25	15	24
2	25	21	34	16	26
3	50	40	58	31	48
4	75	57	98	46	57
5	100	77	132	58	69
6	150	108	188	90	100
7	Average Time	53.33	89.16	42.66	54.00

Although, figure 2 is the graphical representation of the results.

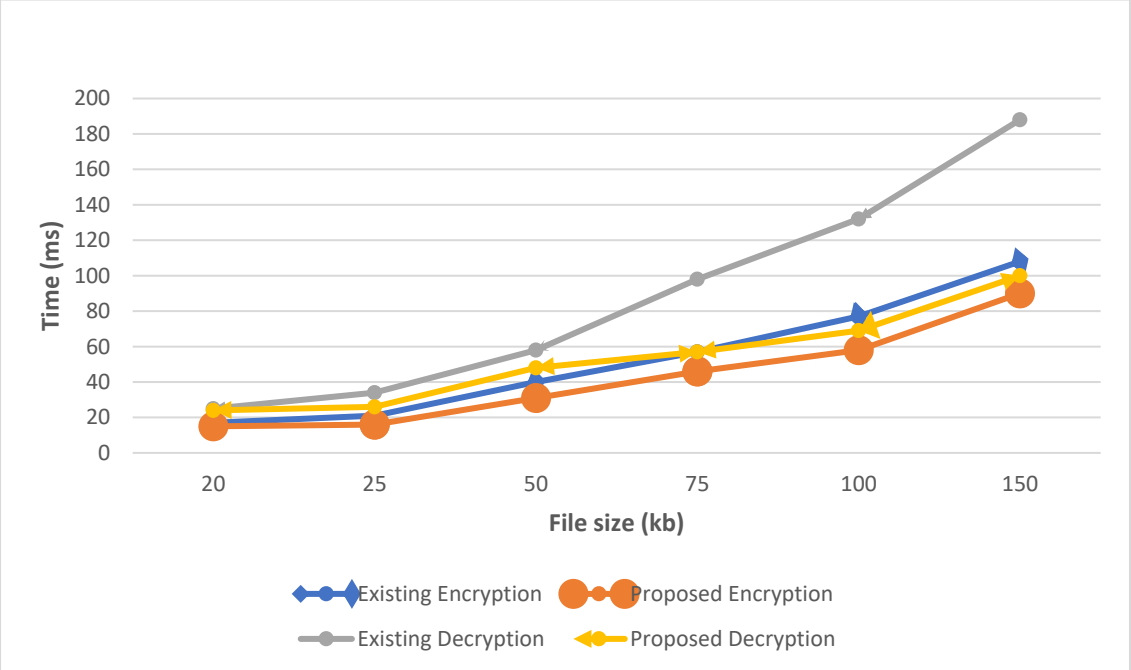

Figure 2: Graphical representation of an Image-file Encryption & Decryption Time.

CONCLUSION

In conclusion, the goal of this paper is to minimize and safeguard the data security threats that is facing MCC by proposing hybrid algorithm that enhanced the system. Although this research does not cover the entire sphere of cloud computing, it tries to improve the data security in terms of integrity and confidentiality so that the existing method should to be re-

structured and re-organized in such a way that will be effective, efficient and secured. However, the proposed method tends to eliminate some of the complexities associated with the existing methods.

REFERENCES

1. Kemp, S. (2019). *Digital 2019: Global internet use accelerates.* New York: Global digital reports.
2. Turner, A. (2020). *The global risks report.* Geneva: World economic forum and Marsh McLennan.
3. Keke Gai, M. Q. (2015). Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. *Security and communication networks*, 1-10.
4. Bhargava, B. (2013). End-to-End Security in Mobile-Cloud Computing. *Education and Research in Information Assurance and Security*, 5-7.
5. C. Donald, S. A. (2013). Mobile Cloud Security Issues and Challenges. *Journal of Information Communication Technology*, 401-406.
6. Hoang T. Dinh, C. L. (2011). A survey of mobile cloud computing: Architecture, applications, and approaches. *International Journal of Wireless Communications and Mobile Computing*, 1587-1611.
7. Kimberly, M. (2021, August 4). *Statista*. Retrieved from statista.com: http://www.statista.com/about us/our-research-commitment/2791/kimberly-mlitz.
8. Richardson, R. (2020). *Computer crime and security survey.* Florida: Computer security institute.
9. Stewart, A. (2005). Information Security Technologies as a commodity input. *Information Management & Computer Security*, 5-15.
10. A. Vichare, J. T. (2017). Data Security using Authenticated Encryption and Decryption Algorithm for Android Phones. *International Conference on Computing, Communication and Automation (ICCCA)* (pp. 50-62). Chicago: Greater Noida.
11. E. J. Kusuma, C. A. (2018). A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography. *Journal of ICT Research and Applications*, 103-122.
12. Prajapati, R. (2021, July 17). *Quora*. Retrieved from Quora: http//:www.quora.com
13. Pooja, R. P. (2020). Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images. *International Research Journal of Engineering and Technology (IRJET)*, 3773-3778.
14. Suba Rani, N. M. (2019). An Image Encryption & Decryption and Comparison with Text - AES Algorithm. *International journal of scientific & technology research*, 668-673.
15. Pittalia, P. P. (2019). A Comparative Study of Hash Algorithms in Cryptography. *International Journal of Computer*

Science Mobile Computing, 147-152.

16. Ahmed Mohammed Saba, I. S. (2018). Software implementation of advanced encryption standard (AES) with graphical user interface using visual studio net. *Journal of Electrical Engineering and Technology*, 1-14.
17. K. K. Saraf, N. G. (2018). Text Encryption and Decryption using AES Algorithm. *International Journal of Electronic Computer System*, 638-643.
18. Israa H. Latif, E. E. (2017). Implementation of Hybrid Cryptosystem using AES-256 and SHA-2 256 by LabVIEW. International Journal of Advanced Research in Computer and Communication Engineering, 352-357.
19. S. Aruna Sankaralingam, G. A. (2018). A hybrid cryptographic algorithm based on AES and SHA in RFID. International Journal of Pure and Applied Mathematics, 835-840.
20. Prajapati, R. (2021, July 17). Quora. Retrieved from Quora: http//:www.quora.com
21. Richardson, R. (2020). *Computer Crime and Security Survey.* Florida: Computer Security Institute.