International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1099-1104 www.ijaem.net ISSN: 2395-5252

Sustainable Computing in Mobile Platform

Pankaj kumar S Thakre
Lecturer
Department of Computer Engineering Government Polytechnic,Nagpur, Maharashtra

Submitted: 15-10-2021 Revised: 26-10-2021 Accepted: 28-10-2021

ABSTRACT— With the growth of Cutting-Edge Technologies in the field of IT, development must have to focus on Sustainable Computing with latest models of Cloud Computing, applications based on Internet of Things, Artificial Intelligence and Mobile Technologies. Sustainable Computing is a set of principles that embraces a range of policies, procedures, programs, and attitudes that run the length and breadth of any use of information technologies.

The proposed system secures the data on mobile prior to transmission to cloud Platform. The algorithm deployed is the symmetric key algorithm known as Modern Encryption Standard-II, an effective encryption method to encrypt and decrypt the input file. The method incorporates the Modified Generalized Vernam Cipher method with feedback with different block size from left to right. The entire content is divided into two files and then combined by taking first the second half and then the first block. The method is then similarly recursively applied for different block size from left to right. The results clearly indicate that the method is free from standard cryptography attack such as known plain text attack, differential attack and brute force attack. Extensive security and performance analysis shows that the proposed MES-II algorithm is a highly efficient solution to overcome the security problems.

Keywords—AI,Cloud; Data security; Android

I. INTRODUCTION

The growing field of cloud computing supply mobile users the ability to store data in the cloud Such as google Drive, Drop box etc. By using this application user can uploads their data and download their data from the cloud at any time. It simplifies the limited storage capacity problem of the user. The recent rapid growth of Data over the Internet through mobile devices increases security issues. The Cloud storage Security is one of the most important issue., most of the user uses mobile device which uses android application. Data from Mobile are uploaded in Cloud. To improve the Security issue of users data in the cloud, we introduced an adaptive and dynamic data encryption method to encrypt user data in the mobile phone before it is uploaded by using an algorithm Modern Encryption Standard Version II (MES-II). security policies and technical ways . But user trust himself only rather than service provider hence by encrypting the data before uploading in the cloud provides the security of data.

II. LITERATURE SURVEY

A. Cloud Computing

Cloud computing [1]-[2] is a model generally defined as the clusters of scalable and virtualized resources like distributed computers, storage, and system software etc. which

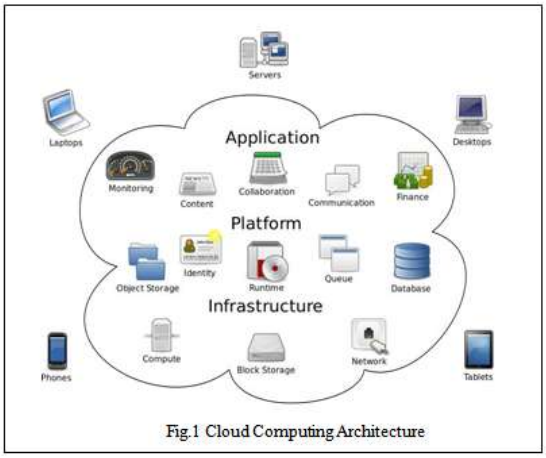

Fig.1 Cloud Computing Architecture

B. Various Security algorithms and technics

Statistics [18][19] shows that 22% of PDA owners have lost their devices, and 81% of those lost devices had no protection. Even worse, 37% of PDAs have sensitive information on them, such as bank account information, corporate data, passwords, and more. For this reason, some companies do not allow employees to use PDAs or similar mobile devices to store company data hence

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1099-1104 www.ijaem.net ISSN: 2395-5252

there is need of effective protection of device sensitive data even if it is stolen or losses.

Hence the author proposes a Self-Encryption scheme[18] for mobile data security.In this scheme the sensitive data is broken into two parts using our self-encryptionstream cipher scheme. The major part (Part A: ciphertext) is stored in the mobile device carried by the company employee, and the minor part (Part B: keystream + other parameters) is protected in the secure server of the company. Part A is encrypted using part B. When the user needs to access the data, he or she has to input a correct PIN to pass the authentication procedure. Then the server will send part B to decrypt part A and merge them together to recover the original plaintext. When a mobile device is lost,at most the adversary can access the part A, from which it is computationally infeasible to get meaningful information.

According to [15][16],author proposed a technic called Location-Dependent Data Encryption in which the mobile client transmits a target latitude/longitude coordinate for data encryption to information server. Then, the server encrypts the message and sends the ciphertext back to the mobile client. The client can only decrypt the ciphertext when the coordinate acquired form GPS receiver matches with the target coordinate. The above technic uses TD(Tolerance Distance) to make accurate coordinate matching because there is no guarantee that the target coordinate matches every time.

According to [21] the top 74% challenges in cloud computing is security. There are many security issues in mobile cloud computing like data ownership, privacy, data security and data segregation. Author proposes a scheme called Homomorphism which is an encryption schemes which allow computing with encrypted value without decrypting them.

According to authors Sebastian Zi ckau,Felix Beierle and Iwailo Denisow[22] a mobile device app is used to access and alter the meta information. Attribute-based encryption mechanisms secure the private data and define access policies for friends and other users simultaneously. The author work on the attributes like ABE information, general meta information, application-specific meta information, access history and file content. The system shows the client is an Android device which provides functionality of Master key, private key and also encryption and decryption.

In Adaptive and dynamic data encryption method[10] for each encryption by user mobile device the algorithm is adaptively and dynamically selected from the algorithm set which is already added in advance in the mobile phone encryption system. The method uses mobile phone hardware information and key selection module responsible to make a dynamic encryption key for data in mobile. And further the modules responsible for dynamically and adaptively selecting the encryption algorithm from set of new high-performance encryption algorithm and generating the encryption key based on the output from the mobile phone hardware information and user personalization information collection module and the input pseudo-random number.

Name of Algorithm /Method	Level of Encryption Strong /Medium	Type of Cryptography Symmetric/ Asymmetric	Efficiency in Encryption /Decryption
Adaptive and dynamic data encryption method	Medium	Symmetric	Max. time spent to select adaptive algorithm from set of algorithms
Multiservice authorization over Mobile Cloud	Strong due to multiple authorization	Asymmetric	Maximum time spent only for multiple authorization
Homomorphic encryption	Medium	Symmetric	Very complex to work on encrypted text hence no specific time for encryption
Attribute-based encryption mechanism	Medium	Symmetric	Efficient but not reliable
Modern Encryption Standard (MES-	Strong due repeated methods	Symmetric	No extra time spent hence efficient but less than MES-II

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1099-1104 www.ijaem.net ISSN: 2395-5252

I)version-I			
Modern Encryption Standard (MES-II)version-II	Very Strong due to bit level	Symmetric	Very efficient takes time in seconds
Location-Dependent Data Encryption	Strong	Asymmetric	Not specific due to distance tolerance problem of location matching
Self-Encryption scheme	Strong	Asymmetric	Procedure Takes time in seconds

Table 1: Comparison of various Security Algorithms with respect to efficiency, level of encryption and type

C. Andriod device and mechanism for security

Android has two basic methods of security enforcement [26]-[30]. Firstly, applications run as Linux processes with their own user IDs and thus are separated from each other. This way, vulnerability in one application does not affect other applications. Since Android provides IPC mechanisms, which need to be secured, a second enforcement mechanism comes into play. Android implements a reference monitor to mediate access to application components based on permission. If an application tries to access another component, the end user must grant the appropriate permissions at installation time. Hence the Android provides more security than other mobile phone platforms. Different levels of data security for different users. It does also embody the concept of cloud computing on- demand services

With respect to author P Nayadkar [24]-[25], there is need to make secured backup and restore of data on Android devices as every person uses it.Here author proposes the system which provide automatic backup and restore of data from mobile online using AES 128 algorithm which is suited at the transmission level. The encrypted file is generated after backup. The system provides online backup and privacy of data in scheduled basis like daily, weekly or monthly. The system developed using Java eclipse and supports backup of bookmarks, contacts, call log, phonebook, SMS, images, videos etc. The author talks about various types of backup technics like Full backup, Incremental backup, Online backup and offline backup etc. Also as per survey by author it is easy to back up our contacts to Google account with Android phone.

III. PROPOSED WORK

To achieve the objective of this system, we have proposed a system which will use Modern Encryption Standard II Algorithm(MES-II) for encrypting and decrypting the data using mobile ID which takes the hardware information of mobile . The MES-II is an algorithm used in Cryptography which focus on how one can achieve high order data security while transmitting from one place to another place.

The method used Modified generalized Vernam cipher method with different block size from left to right and after that entire content is divided into two files and then combine them by taking 2nd half first and then 1st block .The generalized modified Vernam Cipher method again applied from left to right with different block sizes.

The present method on various types of plain text files and the result shows the method is free from standard cryptography attacks namely brute force attack, known plain text attack and differential attack. MES –II can be used as independent encryption algorithm to encrypt any Text data i.e. a file. By using this algorithm we will provide the security of data stored in cloud by means of encryption and decryption process.

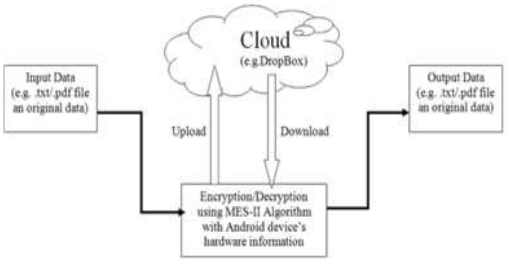

Fig.2 Proposed System Architecture

- Module I: Encryption Module

Module implements encryption of file using MES-II algorithm.Here one PDF or Text file will be converted to temp1 file.The alogorithm uses input as file1 and convert the file1 into encrypted text and written into file called temp1.

- Module II: Decryption Module

Module implements decryption of file using MES-II algorithm.Here Text in filet is decrypted using the index values in key_indx and stored in file2

- Module III :

In this module work on uploading of encrypted file in cloud and downloading it from the cloud is

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1099-1104 www.ijaem.net ISSN: 2395-5252

represented using DropBox.

A) Encryption Module
The algorithm used for encryption of file as given below.
Start main
e_flag=1
Input fi1e1 to plain text file
Input file2 to store cipher text file Open file1 in read mode
Open file2 in write mode file_len=sizeof(file1)
Initialize all elements of array key_indx(row)=0 where row=file_len
Input file_key // User has to enter file_key of any length
Open file _file_key.txt‘ in write mode key_len=length(file_key)
Open a file _temp1.txt‘in write mode Copy _file1‘ to _temp1.txt‘ times=key_len
Initialize all elements of array order(row)=0 where row=times
i=1
random_num= tictoc(1,3) //random_num stores any arbitrary value between 1 and 3
order(i)=random_num
key_indx=keygen(file_key,file_len)//key_indx stores the index values of the generated keypad
Step 18: Call randomizing_key(key_indx,file_len) //randomizing_key stores reshuffled values of key_indx j=1

ch=char(key_indx(j)), write ch to file_key.txt
j=j+1
if j<=file_len then goto step-20 Call Vernam_Cipher_with_Feedback_Encryption(filet,file2,key
_indx)
//this a call to the encryption function. Text in filet is encrypted using the index values in key_indx and stored in file2
Call filecopy(file2,filet) // copying file2 into filet where filet is a temporary file
Step 24: Call filereverse(filet) // To reverse the contents of filet
Call filesplitting(filet,e_flag)// It splits filet into 2 files say file_1 and file_2.
Call mergefile(filet) // this concatenates contents of file_1 to the end of file_2 and stores it in filet i=i+1
If i<=times then goto step15.
Call filecopy(filet,file2) //this copes the contents of filet into file2 .Close all files
Delete temporary files
_temp1.txt','temp_rev.txt','split_file1.txt','split_file2.txt' End

B) Decryption Module
Start main e_flag=0
Initialize all elements of array key_indx(row)=0 where row=file_len
Input fi1e1 to cipher text file Input file2 to store plain text file Open file1 in read mode
Open file2 in write mode
Open a file _temp1.txt‘in write mode Copy _file1‘ to _temp1.txt‘
Open file _file_key.txt‘ in write mode key_pos=0
i=times num=order(i)
Call filesplitting(filet,e_flag)// It splits filet into 2 files say file_1 and file_2.

Call mergefile(filet) // this concatenates contents of file_1 to the end of file_2 and stores it in filet
Call filereverse(filet)// To reverse the contents of filet
key_pos=key_pos+file_len
Move the file pointer in file _file_key.txt‘ to position –key_pos from the end
j=1
ch=read character from _file_key.txt‘,convert to its ASCII code and store it key_indx(j)
j=j+1
if j<=file_len then goto Step-18
Call Vernam_Cipher_with_Feedback_Decryption(filet,file2,key_indx) //this a call to the decryption function. Text in filet is decrypted using the index values in key_indx and stored in file2
Call filecopy(file2,filet)//this copes the contents of file2 into filet
i=i+1
If i<=times then goto Step-11
Call filecopy(filet,file2)//this copes the contents of filet into file2
Close all files
Delete temporary files
_temp1.txt','temp_rev.txt','split_file1.txt','split_file2.txt'
End

IV. RESULT AND CONCLUSION

We compared the system on Android Mobile using various technic. After adding file size of 1MB to 10MB the system shows very efficient result for MES-II.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1099-1104 www.ijaem.net ISSN: 2395-5252

File size	Attribute-Based	Location Based	Self-Encryption	MES-I	MES-II
1MB	6	8	6	4	3
2MB	8	9	7	6	4
4MB	8	9	7	6	5
10MB	26	32	20	18	10

Table2: Comparison of Execution time in second

Fig.3 Screenshot of Android Mobile App.

The above system uses the new symmetric key cryptographic method (MES-II) hence it will keep the size of resulting encrypted text same or less.

Hence the proposed system is very efficient for long message cryptosystem and provides strong security of data over cloud. As the size of encrypted text is not vary from original text hence the technic will provides efficient and better performance. The given technic will not select the specific algorithm from the set of algorithms hence it saves time to process. The System will be free from standard cryptography attack such as plane text attack, brute force attack and differential attack. Hence from all the merits of proposed technic used for making the system, the security of data for users of android devices will be enhanced for cloud.

REFERENCES

[1] John Viega, "Cloud Computing and the Common Man", Computer, vol.42, no. 8, pp. 106-108, August 2009, doi:10.1109/MC.2009.252.

[2] ENISA: Cloud Computing: Benefits, Risks and Recommendations for Information Security. Tech Rep., European Network and Information Security Agency[EB/OL]. [2009-11-20]. http:// enisa.europa.eu.

[3] Molnard D, Schechter S. Self-Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud[C]// Proceedings of Workshop on the Economics of Information Security (WEIS 2010): June 7-8, 2010.Harvard University, MA, USA, 2010.

[4] Ms. Disha H. Parekh, Dr. R. Sridaran , ―An Analysis of Security Challenges in Cloud Computing‖ (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013

[5] Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications 34.1 (2011): 1-11.

[6] CSA: Cloud Security Guide. Tech. Rep., Cloud Security Alliance[EB/OL]. [2009-04]. http://www. cloudsecurityalliance.org/csaguide.pdf.

[7] Reddy, A. Rama Mohan. "Data Security in Cloud based on Trusted Computing Environment."

[8] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou ‖Ensuring Data Storage Security in Cloud Computing‖, Cong Wang, Qian Wang, and Kui Ren and Wenjing Lou ,978-1-4244-3876-1/09/$25.00 ©2009 IEEE

[9] Xiao Zhang, Hong-tao Du ,Jian-quan Chen, Yi Lin, Lei-jie Zeng," Ensure Data Security in Cloud Storage"2011 International Conference on Network Computing and Information Security.

[10] CAO Wanpeng1, BI Wei2, ―Adaptive and Dynamic Mobile Phone Data Encryption Method‖, Communications, China (Volume:11 , Issue: 1),IEEE, May 2014.

[11] ―Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method‖, Somdip Dey, Asoke Nath, Proceedings of IEEE 2nd World Congress on Information and Communication Technologies (WICT-2012), pp. 242-247.

[12] Gunjan Sekhon,Asoke Nath, ―Modern Encryption Standard (MES) Version-II‖, Proceedings of IEEE International Conference on Communication Systems and Network Technologies,April 2013.

[13] Symmetric key Cryptosystem using combined Cryptographic algorithms-Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm, proceeding of information and Communication Technologies(WICT),2011 held at Mumbai Dec 2011,Pages:1175-1180.

[14] Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm: , Jounal of Computing, Vol 3, issue-2, Page 66-71,Feb(2011).

[15] LIAO H C, LEE P C, CHAO Y H, et al. A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security[C]// Proceedings of the 9th International Conference on Advanced Communication Technology:February 12-14, 2007. Gangwon-Do,Korea, 2007: 625-628.

[16] LIAO H C, CHAO Y. H. A New Data Encryption Algorithm Based on the Location of Mobile Users[J]. Information Technology Journal, 2008, 7(1): 63-69.

[17] BAO Haiyong, WEI Guiyi, SHAO Jun, et al. Efficient Signature- Encryption Scheme for Mobile Computation[C]// Proceedings of 2011 International Conference on System Science and Engineering (ICSSE): June 8-10, 2011. Macao, China, 2011: 390-393.

[18] Yu Chen and Wei-Shinn Ku ―Self-Encryption Scheme for Data Security in Mobile Devices‖ Manuscript submitted, Oct. 2, 2008 to CCNC'09, Las Vegas, NV,USA, Jan. 10 – 13, 2009.

[19] GASTI P, CHEN Yu. Breaking and Fixing the Self Encryption Scheme for Data Security in Mobile Devices[C]// Proceedings of 2010 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing (PDP): February 17-19, 2010. Pisa, Italy, 2010: 624-630

[20] Mr. Falesh M. Shelke , Prof. Pravin D. Soni ,―An Enhanced Authentication Strategy for Multiservice Authorization over Mobile Cloud‖ International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue:1

[21] ―Homomorphic Encryption in Mobile Multi Cloud Computing‖ by Maya Louk and Hyotaek Lim 978-1-4799-8342-1/15/$31.00 ©2015 IEEE.

[22] Sebastian Zickau, Felix Beierle, and Iwailo Denisow ,―Securing Mobile Cloud Data with Personalized Attribute-based Meta Information‖ 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering 2015

[23] ‖ Review on Android and Smartphone Security‖, Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh NRI Institute of Information Science and Technology, Bhopal,Madhya Pradesh, INDIA, Received 25th October 2013, revised 4th November 2013, accepted 19th November 2013

[24] Pratap P.Nayadkar, Balu L.Parne. ―A Survey on Different Backup and Restore Techniques Used in Mobile Devices‖ IJCSIT issue 6,vol 5,issn:0975-9646.

[25] Pratap P.Nayadkar ,"Automatic and Secured Backup and Restore Technique in Android",IEEE International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS'15),March 2015

[26] Kaur S. and Kaur M., Review Paper on Implementing Security on Android Application, Journal of Environmental Sciences, Computer Science and Engineering & Technology, 2(3), (2013)

[27] Powar S.,Meshram B. B., Survey on Android Security Framework, International Journal of Engineering Research and Applications, 3(2), (2013)

[28] Bing H., Analysis and Research of Systems Security Based on Android, Intelligent Computation Technology and Automation, 581–584 (2012)