2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)
GLA University, Mathura, UP, India. Feb 28-29, 2020

2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) 978-1-7281-6575-2/20/$31.00 ©2020 IEEE 10.1109/PARC49193.2020.236666

A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique

Anuj Kumar
Department of Computer Engineering and Applications, GLA University, Mathura, India
anujkumar.gla@gla.ac.in

Vinod Jain
Department of Computer Engineering and Applications, GLA University, Mathura, India
vinod.jain@gla.ac.in

Anupam Yadav
Department of Computer Engineering and Applications, GLA University, Mathura, India
anupam.yadav@gla.ac.in

***Abstract*—People store their data on cloud storage very commonly now a day. Security is a major issue in storing data on clouds. Cryptography techniques are very useful to impose security on data. In this paper a hybrid cryptography system is proposed to provide better security on the data which is stored on cloud storage. The proposed approach use RSA algorithm and DES algorithm and provide a hybrid of the two algorithms to provide more security on the data before storing it on cloud. The proposed algorithm is implemented in JAVA and test on a sample plain text. The paper will be very useful for IOT applications storing data on cloud. It is verified that the proposed algorithm is working well to provide more security on data.**

Keywords—Cloud; RSA Algorithm; DES Algorithm; KeyGeneration; Private key; Public key; Secret key; Authentication; Encryption; Decryption

I. INTRODUCTION

Present time is a technology age where different technologies are present in the world. Cloud computing is one of them. it forms an architecture provisioning many it resources as operating systems without direct active management by the user[4]. Infrastructure, software and platform are the services which are provided by this emerging technology. Cloud computing is a method where many group of servers are connected to each other to share many services or resources online. In cloud computing a service (SAAS)[1] .it is a combination of processors and software. It gives us a computing platform where alteration in data perform in all types of computing services on big volume. It provides us a big network and pliability in network connections which makes it very easier to users. By this users can easily used those high quality services from data and provides remote on data storing centers. Data storing on cloud avoids the complexities regarding hardware management of users.[3] Although in comparison of our personal computing devices clouds provide us more powerful and reliable storage services. But in this system a intimidation and fear is always available about our stored data because this data is handle by a CSP (cloud service providers). Data security is most important concern in cloud. This paper focused on issues experienced when the data upload and download from cloud because the quality of service depends on theses task. A new question is arise here how the best services is provide to user in term of data storing and downloading services over cloud. And stored data should be correct irrespective of knowledge about the data. Users can store private data in cloud and security of that data is important issue. Further a new issue also emerges is correctness of data storage in Cloud. There are lot of algorithms are available for data security like symmetric and asymmetric algorithm in cryptography. Bunch of these algorithms contains AES, BLOWFISH, RSA, and DES, triple DES etc. all algorithms are used for data integrity, confidentiality and availability of data which are major concern in cryptography field and for security purpose. In this paper we applied 2 layer of security which makes process of data uploading and downloading more secure. We applied hybrid of RSA and DES algorithm for encryption at the time of data storing in cloud and same algorithms are used in reverse order for decrypting our stored data in cloud when we want to download our data.

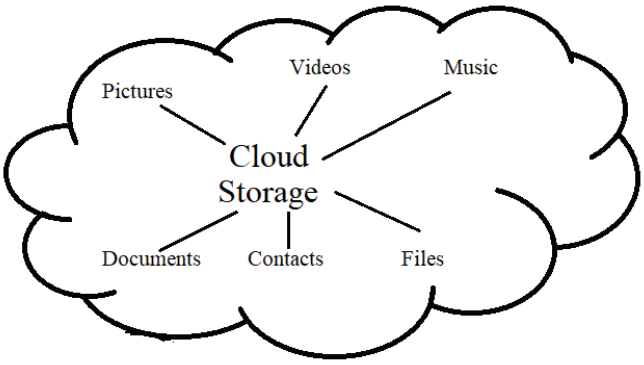

Fig. 1. Cloud Storage

Figure 1 is illustrating a sample of cloud storage which is storing documents, files, contact, videos etc for its users.

Almost every cloud provider does not provide enough security measures to ensure the data safety and that's why clients waver keeping their data at some place which is very easy to be accessed by someone else. Next section illustrate the recent work carried out in security of cloud data storage.

II. LITERATURE SURVEY

V. S. Mahalle and A. K. Shahade [1] applied hybrid cryptography technique for securing data on cloud storage. A hybrid encryption and decryption algorithm using RSA and AES algorithms was proposed. The paper was only focusing on administrative unaware uploading and downloading of data by maintaining its integrity. Further the key distribution was very secure because three keys are distributed for doing encryption and decryption. A unique key generation technique was used to make the process more secure. A. A. Kumar et al.[2]applied two layers of security for cloud data.

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 26,2020 at 13:11:37 UTC from IEEE Xplore. Restrictions apply.

In first layer public key cryptography technique is used where RSA method is used for key exchange and for encryption and decryption author used AES. Second layer of security completely focus on stenography where stumble the encrypted message put on images. A two layer techniques was used to enhance the security of cloud data. Fetching of data without affect was very easy.

K. Saini, et al.[3] applied a new approach for cloud data security. The paper was focusing on drawbacks of functions and in terms of memory size and time of cryptography techniques like AES,RSA,MD5.In this paper Public key was used for Encryption and Decryption was followed by Private key. The important feature of this paper was server could not saw the message and plaintext was never stolen .E2EE was a unique technique used to make process secure.

N. L. Kodumru and M. Supriya[4] applied the bunch of cryptography algorithms RSA, AES and One Time Pad for uploading of data in cloud computing environment. This paper was focus on comparisons of these three Models of security and analyzes them and was found the RSA and OTP was good for storing data in cloud because after analysis author was found the time and space complexity of these algorithm was less as compare to other techniques. Jayapandian, et al.[5] focused on symmetric key cryptography and asymmetric key cryptography technique for providing security in cloud data storage. In asymmetric key cryptography how DES provide security by using a single key and In symmetric cryptography the concept of public and private key was used to make process more secure in cloud data storage explained by author.

P. Yellamma, C. Narasimham and V. Sreenivas[6]applied asymmetric cryptography technique for securing data on cloud storage. A encryption and decryption algorithm using RSA algorithm was proposed. The paper was only focusing on administrative unaware uploading and downloading of data by maintaining its integrity. Further the key generation was very secure in virtual environment for doing encryption and decryption. A key generation technique was used to make the process more secure. K. Pant, J. Prakash and A. Asthana[7] described the issues which were faced in cloud data storage and security in virtual environment and proposed a combination of public key cryptosystem and stenography in cloud data storage and security where explained the encryption and decryption method in virtual environment. P. Gupta et.al[12]proposed a new scheme for data security in cloud. It improves RSA algorithm speed by using multi threading concept. In this work it also compare between other cryptography techniques like RSA AES KP-ABE etc and find proposed algorithm gives better speed as compare to traditional algorithms. I. G. Amalarethinam[13]focused on the time of encryption and decryption process at the time of uploading and downloading from cloud. In this work author solve this problem by using proposed algorithm in which files divided in blocks and enhances the power of algorithm by using enhancement in key.

By going through this literature survey it is observed that there is need to improve the security on the data which is stored on cloud storage. The next section illustrate the proposed approach for storing the data on cloud storage.

III. PROPOSED WORK

This paper uses the hybrid of the RSA and DES algorithms to store the data on the cloud storage. Before uploading data on cloud ,The first step of security apply using RSA algorithm .where data will be encrypted by Rivest Shamir Adhelman (RSA) Algorithm .Following are some advantages of the RSA algorithm which make it very useful:

1. The information which is encrypted and decrypted using RSA algorithm is only accessible to its sender and the receiver. No one in between can access the information.
2. The RSA algorithm ensures that the content that is to be transferred is not altered during the exchange.
3. The information exchanged via RSA algorithm is highly authenticated i.e. only the valid receiver is able to decrypt the information.
4. The private key which is used by the RSA algorithm is unique.

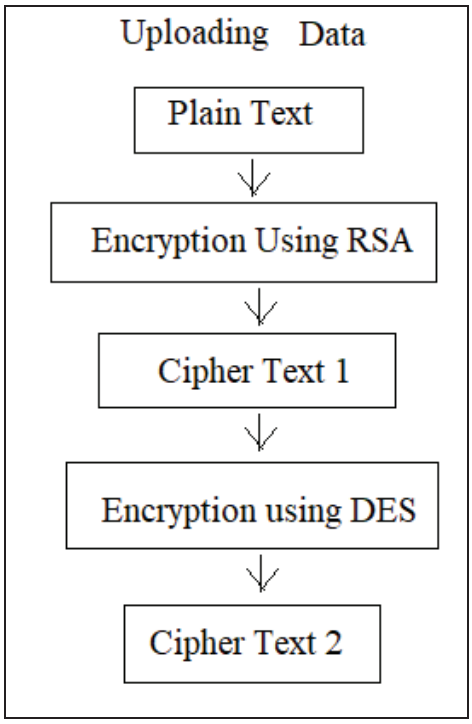

Fig. 2 (a) Uploading data on cloud

The DES algorithm is used with RSA algorithm to make the overall algorithm very secure. In second layer of security we apply Data Encryption Standard Algorithm for encrypted that data which was the output of first stage. after applying DES and RSA algorithm makes more secure for uploading of data in clouds. Following are the features of the DES algorithm which makes it very useful:

1. DES algorithm uses 56 bit keys which make it very unpredictable for the brute force attack.
2. It is very difficult to break because of the confusion and diffusion operations.

In this work a new approach for storage of data in cloud using hybrid cryptography is proposed. Figure 2 (a) is showing the steps of uploading of data on cloud and figure 2(b) is showing the steps of downloading the data from cloud storage.

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 26,2020 at 13:11:37 UTC from IEEE Xplore. Restrictions apply.

The plain text is first encrypted using RSA algorithm and it generate the Cipher Text 1. The Cipher Text 1 is then provided to DES algorithm which generate the Cipher Text 2. The Cipher Text 2 is then stored on cloud storage.

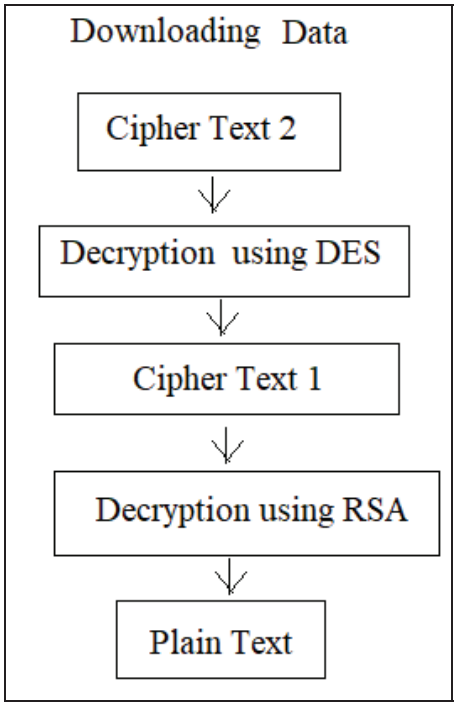

Fig. 2(b) Downloading data from cloud

While downloading the data from cloud storage the Cipher Text is first decrypted using DES algorithm which generate the Cipher Text 1. The Cipher Text 1 is then provided to DES algorithm for decryption which generate the plain text back to the user.

IV. Result and Analysis

In this work, a new security system is proposed using hybridization of RSA and DES algorithms for cloud storage. The proposed approach is implemented in JAVA programming language on a sample plain text. Figure is showing the snapshot of implementation of the proposed approach.

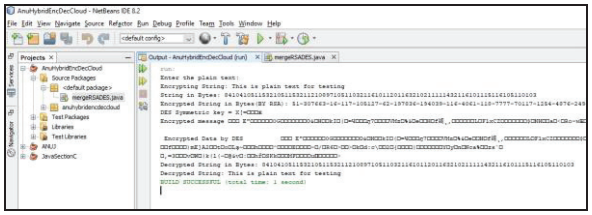

Fig. 3 Snapshot showing working of proposed security architecture for cloud storage

From the figure the it is clear that the hybrid approach can be implemented to encrypt and decrypt the data for storing on the cloud. The next section discusses the limitations and future scope of this work.

V. Conclusion and Future Scope

Security is a very important issue in cloud storage. In this paper a hybrid technique using RSA and DES algorithms is proposed for storage data on clouds. The proposed technique is implemented and simulated on a sample text string of plain text. It is concluded that the proposed technique is more secure as compared to these algorithms when applied alone. But there are some limitations of this work on which work can be done in future which are as follows:

1. These algorithms must be tested on a real environment or on a dedicated simulator.
2. The efficiency in terms of time takes for secure cloud storage should also be measured and compared with other existing techniques.
3. The other combination of cryptography techniques can also be used and tested for the performance.
4. The applicability of the current technique is to be tested on IOT applications.

References

[1] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa&Aes) encryption algorithm," 2014 International Conference on Power, Automation and Communication (INPAC), Amravati, 2014, pp. 146-149.doi: 10.1109/INPAC.2014.6981152

[2] A. A. Kumar, Santhosha and A. Jagan, "Two layer security for data storage in cloud," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Noida, 2015, pp. 471-474.doi: 10.1109/ABLAZE.2015.7155041

[3] K. Saini, V. Agarwal, A. Varshney and A. Gupta, "E2EE For Data Security For Hybrid Cloud Services: A Novel Approach," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India, 2018, pp. 340-347. doi: 10.1109/ICACCCN.2018.8748782

[4] N. L. Kodumru and M. Supriya, "Secure Data Storage in Cloud Using Cryptographic Algorithms," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-6.doi: 10.1109/ICCUBEA.2018.8697550

[5] N. Jayapandian, A. M. J. M. Z. Rahman, S. Radhikadevi and M. Koushikaa, "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-4.doi: 10.1109/STARTUP.2016.7583904

[6] P. Yellamma, C. Narasimham and V. Sreenivas, "Data security in cloud using RSA," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-6.doi: 10.1109/ICCCNT.2013.6726471

[7] V. K. Pant, J. Prakash and A. Asthana, "Three step data security model for cloud computing based on RSA and steganography," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 490-494.doi: 10.1109/ICGCIoT.2015.7380514

[8] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 145-149.doi: 10.1109/BigDataSecurity.2017.12

[9] A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018, pp. 633-636.doi: 10.1109/GUCON.2018.8675033

[10] WenpingGuo, Zhenlong Li, Ying Chen and Xiaoming Zhao, "Security design for Instant Messaging system based on RSA and triple DES," 2009 International Conference on Image Analysis and Signal Processing, Taizhou, 2009, pp. 415-418.doi: 10.1109/IASP.2009.505465

[11] G. Jain and V. Sejwar, "Improving the security by using various cryptographic techniques in cloud computing," 2017 International

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 26,2020 at 13:11:37 UTC from IEEE Xplore. Restrictions apply.

Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 23-28.doi: 10.1109/ICCONS.2017.8250721

[12] P. Gupta, D. Kumar Verma and A. Kumar Singh, "Improving RSA Algorithm Using Multi-Threading Model for Outsourced Data Security in Cloud Storage," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, 2018, pp. 14-15.doi: 10.1109/CONFLUENCE.2018.8442788

[13] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 172-175.doi: 10.1109/WCCCT.2016.50

[14] G. Jain and V. Sejwar, "Improving the security by using various cryptographic techniques in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 23-28.doi: 10.1109/ICCONS.2017.8250721

[15] K. Sinha, S. Choudhary, S. Paul and P. Paul, "Security of Multimedia in Cloud using Secret Shared Key," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018, pp. 908-912.doi: 10.1109/GUCON.2018.8675031

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 26,2020 at 13:11:37 UTC from IEEE Xplore. Restrictions apply.