AN APPROACH TO HYBRID CRYPTOGRAPHY ON CLOUD ENVIRONMENT

Mr. Rohit Barvekar, Mr. Shrajal Behere, Mr.Yash Pounikar, Ms. Anushka Gulhane

Department of CSE PRMITR,Badnera,Amravati,Maharashtra 444606,India

Department of CSE PRMITR,Badnera,Amravati,Maharashtra 444606,India

Department of CSE PRMITR,Badnera,Amravati,Maharashtra 444606,India

Department of CSE PRMITR,Badnera,Amravati,Maharashtra 444606,India

Abstract

Now a day's cloud computing is used in many areas like industry, military colleges etc to storing huge amount of data. We can retrieve data from cloud on request of user. To store data on cloud we have to face many issues .To provide the solution to these issues there are n number of ways .Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing.

This paper presents Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. Security being the most important factor in cloud computing has to be dealt with great precautions. This paper mainly focuses on the following key tasks:

1. Secure Upload of data on cloud such that even the administrator is unaware of the contents.

2. Secure Download of data in such a way that the integrity of data is maintained.

The use of a single key for both encryption and decryption is very prone to malicious attacks. But in hybrid algorithm, this problem is solved by the use of separate keys each for encryption as well as decryption. In this way, both the secure upload as well as secure download of the data is facilitated using the two respective keys.

keywords—*RSA Algorithm,AES Algorithm, Network security, Data Encryption, Decryption, Cryptography, Cloud computing.*

1. INTRODUCTION

Cloud computing has various security issues like data security ,network security, malicious user attacks etc. Users are always concerned whether their data is secure or not. That is why many users do not want their data to be outsourced on cloud. According to a research, in India, there are rarely any organization who make use of big data concepts since they still have everything on papers and they do not have data in the form of spreadsheets or rows and columns. Hardly, any organization here uses big data concepts like hadoop because data is not more than 500 TB, so it could be easily maintained using statistical analysis and tools. Cloud computing is used mainly by Facebook, Amazon and Google [7] as their data is really huge in size which is stored in huge data centres. In future, there will be lot of advancements in this area. Hence, this really motivated us to improve the security mechanisms used for communications [6] which can also be applied in cloud. In this paper, a schema is proposed for ensuring security and privacy of individual data in cloud along with the enhancement of the security mechanism like RSA [4] using Hybrid Encryption RSA and Advanced Encryption Standard (AES).

There are mainly three processes: Key generation, encryption and decryption. The goal is to minimize the running time and cost during these three processes. addition to that, a dual encryption process has been implemented in this algorithm to prevent general attacks against RSA algorithm such as Brute Force, timing and mathematical attacks. In Brute Force attack, the attacker tries to make attempts to guess the private key by generating all the possible combinations. In RSA [2], there is a high chance of guessing the combination until and unless the exponent size is made higher than 2048 bits whereas in the proposed algorithm, the probability is reduced if the exponent size is 1024 bits and more. Moreover, this paper also contrasts between Hybrid Encryption-RSA, asymmetric key cryptographic RSA and symmetric key cryptographic AES in terms of security, efficiency, performance and the above mentioned attacks. Though cloud has many advantages, it has some disadvantages as well, and one of them is security issue. Cloud computing has a number of security issues such as data access control, identity management, risk management, auditing and logging, integrity control, infrastructure and dependent risks. If any organization is using cloud computing, they should provide their important data to service provider. The possibility of sensitive information going to wrong hand is increasing due to cloud services being easily accessible and available for all. The organizations cannot take risks with their sensitive information. Hence, there is a need to resolve the security issue of cloud computing. To solve the data security and privacy issue in cloud computing number of methodology is introduced. There are many risk management is defined. Different ideas or solutions are applied in cloud computing. One of the solutions for data security and integrity problem is encryption.

2. SECURITY ISSUES IN CLOUD

Cloud computing comes with numerous possibilities and challenges simultaneously. Security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast. In terms of customers personal or business data security, the strategic policies of the cloud providers are of highest significance. Security issues in cloud:

- Lack of trust
- Multi-tenancy
- Loss of Control

At highly sensitive data, if we use cloud high degree of security is required for our data. For hosted clouds, third party is responsible for storing and securing data. But is third parties trust worthy? Handing over sensitive data to other party is a serious concern. Data loss is also possible in cloud. A malicious hacker might delete a Target's data out of spite or data can be lost because of a careless cloud service provider. Trusting a third party requires taking the risk of assuming that the trusted third party will act as it is expected (which may not be true all the time). The scalable nature of cloud has posed another threat. Cloud service providers share infrastructure, platforms, and applications to provide services. There is no strong isolation. Two companies might be using same piece of hardware without knowledge. Another question comes who is responsible for security of data? Is it only cloud service providers duty or stake holders, business entities are also responsible for maintaining safeguards. Legal decisions will ultimately determine who owns the responsibility for securing information shared within clouds [2].

3. RELATED WORK

In 2011, Ling Zheng et al. [9] contrasting private cloud and open cloud , records contrasts in the middle of them and advances a building design of private distributed computing to bolster savvy brace, explains structure of every layer, and shows idea of private distributed computing working framework and system virtualization. It gives the hypothetical reference to assemble the private distributed computing, in this way advances the development of the keen network.

In 2011, Ming Li et al. [10] displayed a contextual analysis utilizing online Personal Health Record (PHR), they first demonstrate the need of pursuit ability approval that lessens the security presentation coming about because of the list items, and set up a versatile structure for Authorized Private Keyword Search (APKS) over scrambled cloud information. They then propose two novel answers for APKS in light of a late cryptographic primitive, Hierarchical Predicate Encryption (HPE). Their answers empower proficient multi-dimensional catchphrase seeks with reach inquiry; permit designation and renouncement of pursuit abilities. They upgrade the inquiry protection which shrouds clients' question catchphrases against the server.

In 2011, Yanjiang Yang et al. [11] propose that Storage-as-an administration is a crucial part of the distributed computing framework. Database outsourcing is a run of the mill use situation of the distributed storage administrations, wherein information encryption is a decent approach empowering the information proprietor to hold its control over the outsourced information. Searchable encryption is a cryptographic primitive taking into consideration private watchword based pursuit over the scrambled database. The setting of big business outsourcing database to the cloud requires multi-client searchable encryption, while for all intents and purposes every single existing plan consider the single-client setting. To connect this crevice, they propose a down to earth multi-client searchable encryption plan, which has various points of interest over the known methodologies.

In 2011, Wang et al. [12] proposed that distributed computing has been imagined as the cutting edge building design of IT Enterprise. It moves the application programming and databases to the concentrated extensive server farms, where the administration of the information and administrations may not be completely dependable. A creator concentrates on the issue of guaranteeing the respectability of information stockpiling in Cloud Computing. Specifically, they consider the assignment of permitting an outsider inspector (TPA), for the benefit of the cloud customer, to check the trustworthiness of the dynamic information put away in the cloud. The presentation of TPA kills the association of the customer through the evaluating of whether his information put away in the cloud is for sure in place, which can be essential in accomplishing economies of scale for Cloud Computing.

In 2012, Syed Naqvi et al. [13] present a formal method for testing the effect of adaptability and heterogeneity on the united Cloud security administrations. Their expects to build up a mean of measuring the effect on security capacities under different working conditions and parameters of unified Cloud arrangements. Their aftereffects of this work will assist organizations with identifying the best security structural planning that will fit their Cloud architectures and execution prerequisites.

In 2012, Huaglory Tianfield et al. [14] present an exhaustive study on the difficulties and issues of security in distributed computing. They first investigate the effects of the unmistakable attributes of distributed computing, to be specific, multi-tenure, versatility and outsider control, upon the security prerequisites. At that point, they dissect the cloud security necessities regarding the principal issues, i.e., privacy, respectability, accessibility, trust, and review and consistence. They talk about the scientific categorization for security issues in distributed computing. They outline the security issues in distributed computing by cloud security building design.

In 2012, Abdullah Abuhussein et al. [15] recommend Healthcare, training, business, and numerous different areas take a gander at distributed computing as a try to comprehend the ceaseless deficiency in volume, foundation, availability, and observing strength. On the other hand, moving information to the cloud suggests moving control of the client's information to the cloud administration supplier inconclusively. Thus, the security and protection of the client's data turns into an essential issue. Surveying and looking at among potential distributed computing administrations, represents an issue for learner clients intrigued to move their work to the cloud to pick security choices that are adequate and hearty in the meantime. They endeavors to recognize and classify a rundown of characteristics which mirror the different parts of cloud security and protection. These credits can be utilized to survey and analyze distributed computing administrations with the goal that customers can settle on accomplished decisions. Cloud administration suppliers can utilize them to fabricate and/or offer better cloud arrangements.

In 2012, Wentao Liu et al. [16] propose that the security issue of distributed computing is vital and it can keep the fast improvement of distributed computing. It presents some distributed computing frameworks and breaks down distributed computing security issue and its procedure as indicated by the distributed computing ideas and characters. The information protection and administration accessibility in distributed computing are the key security issue. Single security technique can't tackle the distributed computing security issue and numerous conventional and new advances and methodologies must be utilized together to protect the aggregate distributed computing framework.

In 2014, Nikhilesh Pant et al. [17] present the procedures for cloud appropriation and cloud security appraisal to investigate potential security and consistence suggestions in cloud environment. They talks about in subtle element on how an association may continue for security and consistence appraisal amid the cloud calculation. Their methodology and ideas point by point in this paper would be valuable for associations that are included in the cloud reception process.

In 2015, Liu X. [18] talks about distributed computing information security issues, including tile security of information transmission, stockpiling, security and administration of security. Concentrate on all inclusive information administration influence cloud security examination, and pointed out that a leap forward in the advancement of this distributed computing, attempt to list the comparing methodologies and long haul improvement heading.

In 2016, Gupta et al. [19] has been envisioned as a cutting edge structural planning of IT Industries. Security and protection is the significant obstacle in the cloud environment as a result of its transparent construction modeling. They investigates the cloud security dangers furthermore talks about the current security ways to deal with secure the cloud environment .They additionally proposed a novel Tri-system for cloud security against information break which give all around security to the cloud structural planning.

4. PROPOSED METHODOLOGY

Our proposed approach provides security with two standard encryption mechanisms namely Advanced Encryption Standard (AES) and Ron Rivest, Adi Shamir, and Leonard Adlema (RSA) mechanism.

The proposed system basically consists of two modules

(I) Upload Module

(II) Download Module

(I) Upload Module: It consist of four parts

I. Authentication: User authenticates himself to the Cloud with his unique username and the password.
II. Upload: This module allows user to upload his files in a secure way. Uploads the encrypted form of that data (file) in his document directory of cloud through this gateway.
III. Key Generation.
IV. Encryption: The data after uploading is first stored in the temporary file of the server that is in the Cloud. Then encrypt the data by using the public key of the user and stores the encrypted form of data in the documents of the user.

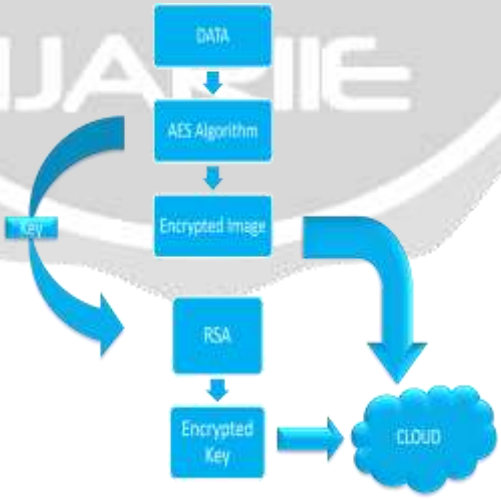

Fig. 1: Encryption Process

(II) Download Module: It consists of two parts

I. Decryption: When user wants to download his secure data, he is prompted to enter his user name along with the secret private key. By using the private key of the user the cloud decrypts the data.

II. Download: Cloud send the Decrypted data to the user thereby giving the user his original data.

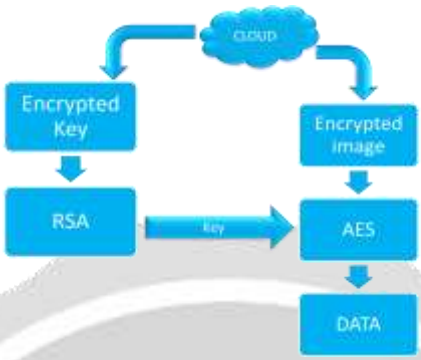

Fig. 2 : Decryption Process

5. ADVANTAGES

Security: The proposed security mechanisms will prevent the confidential data to be misused making the system more reliable.

High speed : The proposed method will make encryption and decryption with proper key much faster than usual.

6. CONCLUSION AND FUTURE SCOPE

An abstract model has been given in the paper which will ensure security and privacy of each user's data in cloud. It has been observed that the difference between the running time of the original RSA and Improved Algorithm using Hybrid Encryption-RSA and AES is increasing drastically. Also, it helped to prevent brute force, mathematical and timing attacks. The main purpose behind using RSA and AES encryption algorithm is that it provides three keys i.e. public key for encryption, and private key and secret key for decryption. The data after uploading is stored in an encrypted form and can be only decrypted by the private key and the secret key of the user. The main advantage of this is that data is very secure on the cloud.

Future work can present a proof of the security for proposed technique, which should focus on the random generation capability of key with the key exchange process.

REFERENCES

[1] Vinita Keer, Dr. Syed Imran Ali, Prof. Neeraj Sharma " Hybrid Approach of Cryptographic Algorithms in Cloud Computing " International Journal of Emerging Technology and Advanced Engineering Volume 6, Issue 7, July 2016

[2] Bhupendra Kumar, Jayshree Boaddh and Lata Mahawar " A hybrid security approach based on AES and RSA for cloud data " International Journal of Advanced Technology and Engineering Exploration Vol 3(17) , 2016.

[3] Punam V. Maitri, Aruna Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm", Wireless Communications Signal Processing and Networking (WiSPNET) International Conference on, pp. 1635-1638, 2016.

[4] Vishwanath S Mahalle and Aniket K Shahade " Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm" Power, Automation and Communication (INPAC), 2014 International Conference"

[5] Mauro Storch, César A. F. de Rose, "Cloud Storage Cost Modeling for Cryptographic File Systems", Parallel Distributed and Network-based Processing (PDP) 2017 25th Euromicro International Conference on, pp. 9-14, 2017, ISSN 2377-5750.

[6] Vikas K. Soman, V Natarajan, "An enhanced hybrid data security algorithm for cloud", Networks & Advances in Computational Technologies (NetACT) 2017 International Conference on, pp. 416-419, 2017.
[7] P Shaikh, V. Kaul, "Enhanced Security Algorithm using Hybrid Encryption and ECC", IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 3, pp. 80-85, May-June 2014
[8] Jasleen Kaur, and Dr. Sushil Garg , "Security in Cloud Computing using Hybrid of Algorithms" ,International Journal of Engineering Research and General Science Volume 3, Issue 5, September October, 2015.
[9] Zheng L, Hu Y, Yang C. Design and research on private cloud computing architecture to support smart grid. In international conference on intelligent humanmachine systems and cybernetics (IHMSC) 2011 (pp. 159-61). IEEE.
[10] Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing. In 31st international conference on distributed computing systems (ICDCS) 2011 (pp. 383-92). IEEE.
[11] Yang Y. Towards multi-user private keyword search for cloud computing. In IEEE international conference on cloud computing (CLOUD) 2011 (pp. 758-9). IEEE.
[12] Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(5):847-59.
[13] Naqvi S, Michot A, Van de Borne M. Analyzing impact of scalability and heterogeneity on the performance of federated cloud security. In IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom) 2012 (pp. 1137-42). IEEE.
[14] Tianfield H. Security issues in cloud computing. In IEEE international conference on systems, man, and cybernetics (SMC) 2012 (pp. 1082-9). IEEE.
[15] Abuhussein A, Bedi H, Shiva S. Evaluating security and privacy in cloud computing services: A Stakeholder's perspective. In international conference for internet technology and secured transactions 2012 (pp. 388-95). IEEE.
[16] Liu W. Research on cloud computing security problem and strategy. In international conference on consumer electronics, communications and networks (CECNet) 2012 (pp. 1216-9). IEEE.
[17] Pant N, Parappa S. Seeding the cloud in a secured way: cloud adoption and security compliance assessment methodologies. In IEEE international conference on software engineering and service science (ICSESS) 2014 (pp. 305-8). IEEE.
[18] Liu X. Data security in cloud computing. In proceedings of the 2015 bv international conference on cybernetics and informatics 2015 (pp. 801-6). Springer New York.
[19] Gupta A, Chourey V. Cloud computing: security threats & control strategy using tri-mechanism. In international conference on control, instrumentation, communication and computational technologies (ICCICCT) 2016 (pp. 309-16). IEEE.