Cloud Computing Security Using RSA & AES

Sweta H Meshram[1] Manisha D Badwaik[2] Chetana N Kore[3] Reshma S Neware[4] Deepak Bhiogade[5]
[1,2,3,4]Student [5]Assistant Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]MPCE Bhilewada, Bhandara, India

Abstract— Presents Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. Security being the most important factor in cloud computing has to be deal with great precautions. This paper mainly focuses on the following key tasks:
1. Secure Upload of knowledge on cloud such even the administrator is unaware of the contents.
2. Secure Download of data in such a way that the integrity of data is maintained.
3. Proper usage and sharing of the general public , private and secret keys involved for encryption and decryption.
The use of one key for both encryption and decryption is extremely prone to malicious attacks. But in hybrid algorithm, this problem is solved by the utilization of three separate keys each for encryption as well as decryption. Out of the three keys one is the public key, which is made available to all, the second one is the private key which lies only with the user. In this way, both the secure upload as well as secure download of the data is facilitated using the two respective keys. Also, the key generation technique used in this paper is unique in its own way. This has helped in avoiding any chances of repeated or redundant key.

Keywords: Cloud computing, AES, RSA, Computing Services

I. INTRODUCTION

Cloud computing is that the results of the evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to al technologies, without the necessity for deep knowledge about or expertise with all of them. The cloud aims to chop costs, and helps the users specialize in their core business rather than being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the method through which the user can provision resources on-demand. By minimizing user involvement, automation accelerates the method, reduces labor costs and reduces the possibility of human errors. Cloud Security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

The conception of cloud computing is associated closely with the infrastructure as a services (IaaS), platform as a services (PaaS), System as a services (SaaS). Cryptography, in modern days is considered combination of three types of algorithms.
They are
1) Symmetric-key algorithms
2) Asymmetric-key algorithms and
3) Hashing. Integrity of data is ensured by hashing algorithms.

A. Public Cloud:

The most recognisable model of cloud computing to many consumers is the model, under which cloud services are provided in a virtualised environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

B. Private Cloud:

Private clouds are those that are built exclusively for a single business. For many companies considering cloud computing, private clouds are a good starting point. They allow the organization to host applications, development environments, and infrastructure in a cloud, while addressing concerns regarding data security and control that can arise in the public cloud environment.

C. Community Cloud:

The cloud foundation is imparted by numerous associations and backings a specific group that has imparted issues (e.g., mission, security necessities, arrangement, and consistence contemplations). Hybrid cloud: A hybrid cloud is generally best-of-breed. It combines the comfort level of a private cloud with the flexibility and versatility of the public cloud. Hybrid platforms use either public clouds or off-site Hosted Virtual Private Clouds for some applications and processes. They merge these with on premises private clouds for high security application environments to leverage the best of both worlds.

II. SECURITY ISSUES OF DATA PRIVACY IN CLOUD

The six issues that must be addressed are:
1) Breach notification and data residency:
2) Data management at rest
3) Data protection in motion
4) Encryption key management
5) Access controls
6) Long-term resiliency of the encryption system

a) Host security issues The host running the job, the job may well be a virus or a worm which can destroy the system from malicious users
b) Network security issues Denial of Service: where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a

certain Internet based service. Like DNS Hacking, Routing Table "Poisoning", XDoS attacks QoS Violation: through congestion, delaying or dropping packets, or through resource hacking. Man in the Middle Attack: To overcome it always use SSL IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address.

c) Security issues from virtualization Type of virtualization provider is using Para Virtualization or full system virtualization. Instance Isolation: ensuring that Different instances running on the same physical machine are isolated from each other. Control of Administrator on Host O/s and Guest o/s. Current VMMs do not offer perfect isolation: Many bugs have been found in all popular VMMs that allow escaping from VM! Virtual machine monitor should be „root secure, meaning that no level of privilege within the virtualized guest environment permits interference with the host system.

d) Ensuring both data and code safety? Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing service provider because the customer generally has no access to the providers facility which can be comprised of multiple facilities spread around the globe.

III. Literature Review

Literature In 2011, Yanjiang Yang et al. [7] 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. [8] 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. [9] 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. [10] 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.

IV. Proposed Work

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. In this approach the enlisted client first chooses the server from the 4 determined previously. Space is overseen for all intents and purposes and it will migrate the space according to the interest by the client with no interference. The information is then transferred in the chose server as asked for by the client and it is then accessible for the self-use reason promptly. The information is then accessible to share to other authorized clients in the cloud from any four servers. For the testing case we have confined the document sort to message just so that legitimate correlation can be given the same kind of information. On the off chance that the enrolled client needs to get to the information of other client, it can be gotten to on solicitation to the specific client through the cloud administration. If the user which is registered in this solicited environment wants to access the data of any other registered user, it can only be permitted through this environment based on the request grant of that particular user not the client. This is the first enhancement of our work. Implies our work gives information offering capacity yet to the safe information exchange. The client information is confined for perspective to the cloud suppliers so information read consent is not for cloud suppliers too. This is the second strength of this work. In the event that the other cloud client consents to share the information to another cloud client then the information is readied for sending it to the regarded cloud client. The information is transferred with AES and RSA mechanism system and the plaintext is changed to content as indicated by AES and RSA both. It provides four key security. This is the next advancement of our work. At that point an information bit document is send with the information that will consequently render the notice to the administration supplier if the not assigned client will open the record first. As the security is by standard encryption strategy it will give a superior and solid against denial of service. This is the third idea included our system. At that point the beneficiary can get

to the information subsequent to applying both AES and RSA encryption standard component. In the event that some other client opens the records the information bit alarms the bungle operation to the cloud supplier. The keys are irregular created so for the same record the keys are distinctive. So following it is distinctive.

V. IMPLEMENTATION

A. Main-Module DFD

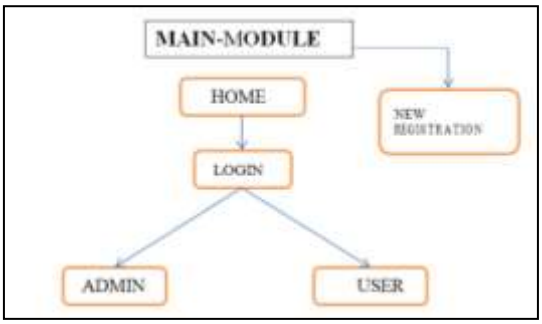

Fig. 1: Main-Module DFD

B. Admin-Module DFD

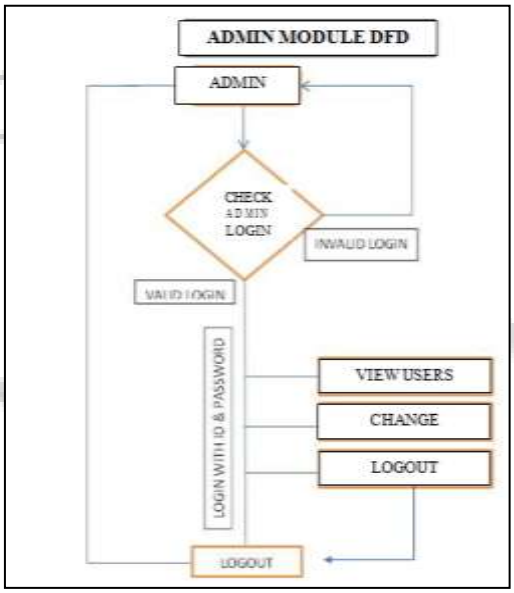

Fig. 2: Admin-Module DFD

C. User-Module DFD:

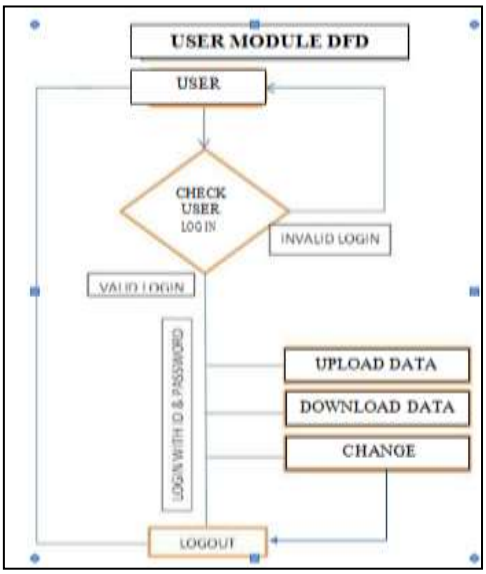

Fig. 3: User-Module DFD

VI. FUTURE SCOPE

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

RAID (originally redundant array of inexpensive disks, now commonly redundant array of independent disks) is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both. Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance.

VII. RESULTS

If user wants to retrieve his personal data, then this page provides download link for accessing his own data. At the time of downloading, System decrypt the user data which is already stored on the server and after that, the data will be provided to the user. And in this way here we have achieved the main aim of our developed system.

Fig. 4: Login Portal (User)

Fig. 5: Login Portal (Admin)

Fig. 6: Admin portal

Fig. 7: User Dashboard

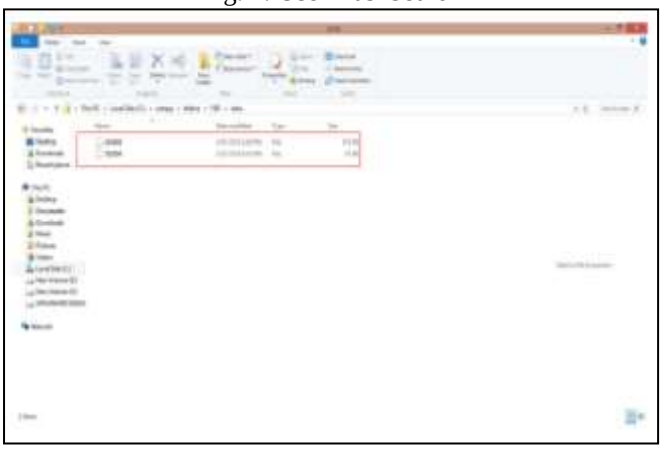
Fig. 8: Store Data in Encrypted Format

VIII. CONCLUSION

From a proper analysis of positive points and constraints on the component, it can be safely concluded that the product has a highly efficient GUI based component. This application is working properly and meeting to all user requirements. This component can be easily plugged in many other systems.

This application software has been computed successfully and was also tested successfully by taking "Test Cases". It is user friendly, and has required options, which can be user to perform the desired operations.

1) Instant access.
2) Improved productivity.
3) Efficient management of data.
4) Simplification of the operations.
5) Less processing time and getting required information.
6) User friendly.

REFERENCES

[1] Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, et al. Above the clouds: A Berkeley view of cloud computing. Department electrical engineer and computer sciences, University of California, Berkeley, Rep. UCB/EECS. 2009; 28(13); 1-42.

[2] Ruiz-Agundez I, Penya YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research. 2012; 2(2); 7-17.

[3] Singh A, Shrivastava M. Overview of security issues in cloud computing. International Journal of Advanced Computer Research (IJACR). 2012; 2(3); 41-5.

[4] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 598-609). ACM.

[5] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering (CONSEG) 2012(pp. 1-8). IEEE.

[6] Juels A, Kaliski Jr BS. PORs: Proofs of retrievability for large files. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 584-97). ACM.

[7] Yang Y. Towards multi-user private keyword search for cloud computing. In IEEE international conference on cloud computing (CLOUD) 2011 (pp. 758-9). IEEE.

[8] 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.

[9] 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.

[10] Tianfield H. Security issues in cloud computing. In IEEE international conference on systems, man, and cybernetics (SMC) 2012 (pp. 1082-9). IEEE.

