Secure Data Storage on Cloud

Mr.Anup Alone[1] Ms.Kirti Gathade[2] Ms.Shunhangi Khobragade[3] Mr.Akshay Yadav[4]
[1,2,3,4]Wainganga College of Engineering & Management, Nagpur, India

Abstract— Cloud computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as services over the internet. With cloud computing technology, users use a variety of devices, including PCs, laptops, smart phones, and PDAs to access programs, storage, and application development platforms over the Internet, via services offered by cloud computing providers. Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. We categorize the existing research according to the cloud reference architecture orchestration, resource control, physical resource, and cloud service management layers, in addition to reviewing the existing developments in privacy-preserving sensitive data approaches in cloud computing such as privacy threat modeling and privacy enhancing protocols and solutions. Our main aim to propose more reliable, decentralized light weight technique for which provides more efficient data security in cloud computing.

Key words: Cloud Computing, RSA Algorithm, Data Security, Storage Process, Encryption, Decryption

I. INTRODUCTION

Organizations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. The Cloud technology is a growing trend and is still undergoing lots of experiments. All business data and software are stored on servers at a remote location referred to as Data centers. Data center environment allows enterprises to run applications faster, with easier manageability and less maintenance effort, and more rapidly scale resources (e.g. servers, storage, and networking) to meet fluctuating business needs[1].

While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons [2]. In cloud computing data and applications are maintained with the use of central remote server and internet and allow consumers to use the applications without installation and also with the help of internet cloud computing allows customers to access their personal files which are stored in some other computer.

II. LITERATURE REVIEW

Cong Wang et.al.[1] has proposed a homomorphic token with distributed verification of erasure-coded data, their scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, their scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server.

Sachindra kumar dubey et. al [2] has proposed an various methods for ensuring the data security on the cloud. An author demonstrate how confidentiality and authentication security can be achieved by using erasure coding and TPM techniques. And the author dealt with the different security methods to protect the data stored in the cloud.

Sudesh sharma et. al. [3] illustrate the homeomorphic encryption algorithm. An algorithm like EcEgamel algorithm for better result and reduced computation time because it uses elliptic curve which reduces the key size to greater extent by providing same security like other algorithm.

Zhibin Zhau and Dijiany Huang [4] has proposed "Efficient and secure data storage operations for mobile cloud computing"

In this, authors has a proposed a holistic security framework to secure the data storage in public cloud with the special focus on lightweight wireless device store and retrieve data without expressing the data content to the cloud service provider.

Durgarajesh Rachamsetty, prof. Ramkrishan Rao TK et. al. [5] has proposed "A process for data storage security in cloud computing".

In this paper they proposed a effective and flexible technique for managing the data storage technology in the secure way, by utilizing the PMAR homorphic encryption algorithm with dispersed authentication of erasure coded data.

By utilizing this technique, it is helpful to achieve incorporation of storage correctness insurance and data error localization

III. EXISTING METHODOLOGY

A. Advance Encryption Standard

a"Implementation of advanced encryption standard Algorithm(AES)" but this system is using symmetric key thats why it cannot secure the system in better way.

Advanced Encryption Standard algorithm is a Symmetric block cipher. In which used only one secret key. The same key is used for encryption as well as decryption. Basically AES standard key sizes are 128 bit, 192 bit and 256 bit. For 128 bit key size. But the data size udes by the AES was not sufficient for computation but this can be solve by the RSA. RSA gives better security than the AES and it has large data size than the AES. RSA use 245 bytes i.e.2048 bits , in this way it can overcome the problem of small data size.

B. Challenge Token Creation

The main idea is - when a file is distributed to the cloud, the user pre-computes a certain number of short verification tokens on individual vector G(j) (j {1, . . . , n}), each token covering a random subset of data blocks that would be distributed to the different cloud servers. Later, when the user

wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. Upon receiving challenge, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. Suppose if the user wants to challenge the cloud server t times to ensure the correctness of data storage, the user must pre-compute x verification tokens for each G(j) (j {1, . . . , n}), a challenge key kchal and a master permutation key KPRP. To generate the ith token for server j, the user acts as follows,

Challenge Token Creation

- 1. Derive a random challenge value) i and a permutation key k(i) *prp* based on *KPRP.*
- 2. Compute the set of r randomly-chosen indices.
- 3. Calculate the token v(j)i using the random challenge value .

Fig. 1: Challenge Token Creation

IV. PROPOSED WORK

A. *User Module*

This module contain the login part for the user. After the login process he can search the files and he can download the files from the cloud. Data user is the authorized one to access the documents of data owner.

B. *Admin Module*

Admin who has expertise and capabilities that users may not have. This module helps the owner to register those details and also include login details. This module helps the owner to upload his file with encryption using RSA algorithm.

1) Activities performed by the Admin are:

– Upload the file on Cloud.
– Report
– Create Employee/Delete employee
– Manage the data

C. *Encryption Module*

This module helps the server to encrypt the documents using RSA algorithm. The cloud server store the encrypted document collection.

D. *Cloud Data Storage Module*

Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data.

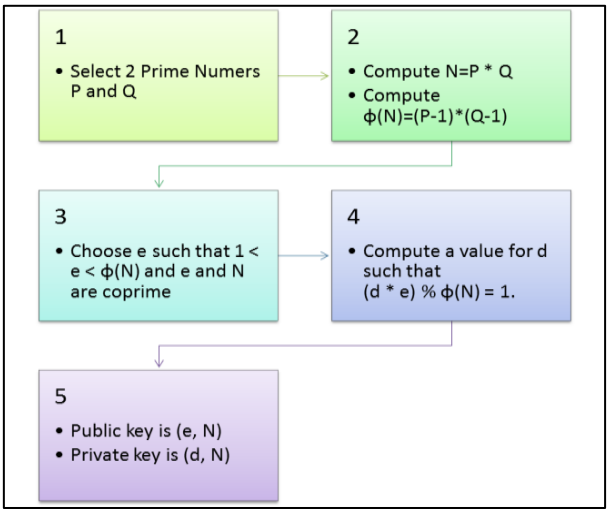

Fig. 2: (RSA) Proposed Algorithm

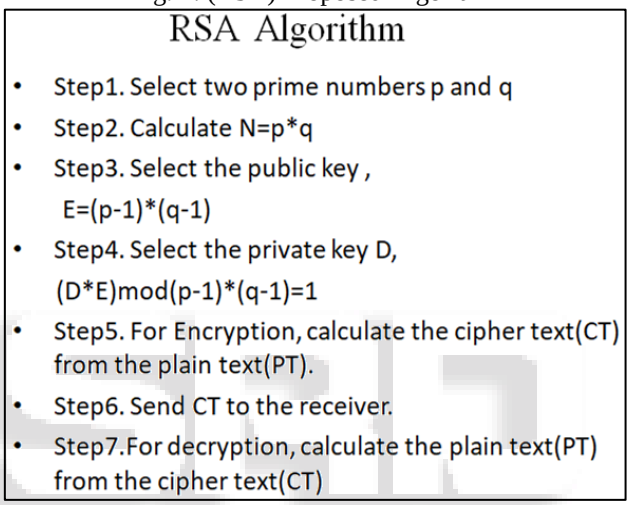

Fig. 3: RSA Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for p and q, the resulting n will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining d without factoring n are equally as difficult.

Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

1) Flow Chart:

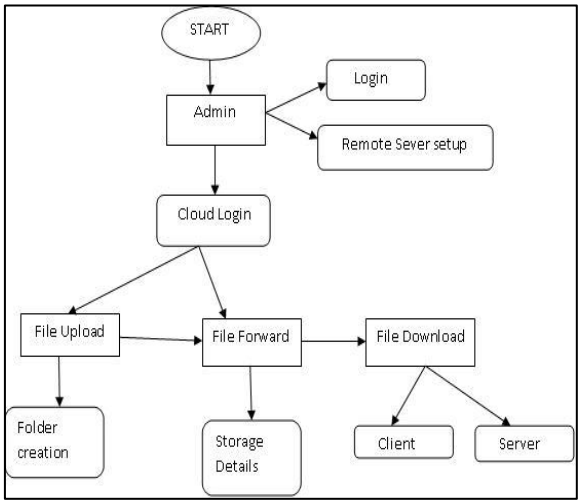

Fig. 2: Proposed Architecture

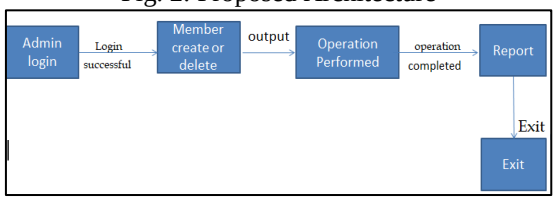

Fig. 3: Data Flow Diagram

Firstly Admin login into the cloud system then create or delete the client/employee. Files are uploaded or forwarded by Admin and downloaded by client. Only authorized user can access or download the data.

V. TECHNOLOGY/TOOLS REQUIRED

Version: PHP (5.5.7)
Database: PHP MySQL 5.5
Operating System: Windows 7.

VI. OUTCOME/ POSSIBLE RESULTS

After the implementation of all modules, it will give the complete reliable system for cloud computing users. This system will helpful for security purpose of data which is stored in the cloud.

VII. CONCLUSION AND FUTURE SCOPE

This synopsis investigates the Data Security concept as an important approach to enhance the security and privacy of stored client's data in cloud computing systems, especially in the public cloud environment where data may be moved frequently from one cloud server to another and may be accessed by other end entities. This study focuses on securing the actual data from possible security risks in the cloud environment without fully relying on trusting the cloud provider or a third party. By contrast, approaches that focus on securing the hardware and applications handling the data in the cloud require the data owner to trust the cloud provider or a third party for providing the desired security and privacy requirements.

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren "in Ensuring Data Storage Security Cloud Computing"Department of ECE Illinois Institute of Technology .
[2] Shachindra Kumar Dubey, Prof. Ashok Verma "DATA STORAGE IN CLOUD COMPUTING" ,June 2013.
[3] Sudesh Sharma and Dr. Karambir " A Review of Security of Data Storage and Retrieval on Cloud using Homomorphic Encryption" , May 2017
[4] Zhibin Zhau and Dijiany Huang "Efficient and secure data storage operations for mobile cloud computing" IJCSIT.
[5] Durgarajesh Rachamsetty, prof. Ramkrishan Rao TK "A process for data storage security in cloud computing". IJCSIT 2011
[6] Wang, Qian,. "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22.5 2011.
[7] Nirmala V., Sivanandhan R.K., and Lakshmi R.S. "Data confidentiality and Integrity Verification using Authenticator",March 2013.
[8] Chuang, I-Hsun, "An effective privacy protection scheme for cloud computing."
[9] Juels and J. Burton S. Kaliski, "PoRs: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
[10] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," Online at https://www.sun. Com/offers/details/sun transparency.xml, November 2009.
[11] M. Arrington, "Gmail disaster: Reports of mass email deletions," online at http: // www. techcrunch.com/2006/12/ 28/gmail-disasterreports-ofmass-email-deletions/, December 2006.
[12] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.
[13] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12, 2006.
[14] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.
[15] N. Gohring, "Amazon's S3 down for several hours,"Onlineat http://www.pcworld.com/businesscenter/article/142549/ amazons s3 down for several hours.html, 2008.
[16] Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files,", 2007.
[17] H. Shacham and B. Waters, "Compact Proofs of Retrievability," 2008.
[18] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theoryand Implementation," Cryptology ePrint Archive, Report 2008

