International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Cloud Data Security and Reliability using RSA and SHA-2 Algorithms - A Novel Approach

VeeraRaghavaRao Atukuri*[1], Dr. Ramineni SivaRamaPrasad[2]

*[1]Research Scholar, Department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

[2]Head of the Department, Department of Commerce and Business Administration, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

ABSTRACT

Cloud computing is a latest and emerging technology in the current IT field. It is very useful technology which it can store the numerous of data in servers and can be accessed from anywhere in the world through Internet. Simply, on demand we can access the resources from Internet at anytime and anywhere. It is the latest architecture of IT industry. It works on the software and large databases where the services are not fully trusted. This poses many security challenges, which have not been well defined and worked. In this paper, we develop a system with strong benefits and strong securities. So whenever a customer storing his data on cloud server he is not worry about his data. The system is developed with a mechanism, which is highly trustworthy in placing the user data in to cloud server and retrieving, by the cloud user.

Keywords : Cloud Computing, Security, on demand

I. INTRODUCTION

Cloud computing is the use of computing resources (software and hardware) that are delivered as a service over a network (Internet). It entrusts remote services with a user's data, software and computation. Cloud computing is a general term for anything that involves delivering hosted services over the internet. A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic-a user can have as much or as little of a service as we want at any given time; and the service is fully managed by the provider. A Cloud can be private or public. A public cloud sells services to anyone on the Internet. Currently, Amazon web services is the largest public cloud provider. [6]. Quality of service is an important aspect from the view point of data security. In Cloud computing there are new challenges towards security threats for various reasons. We cannot directly apply cryptographic techniques for data security protection due to the user losses control of data under cloud computing [2]. Customer stores various kinds of data in the cloud and he wants good assurance of the security of his data. But the problem of verifying correctness of data stored in the cloud becomes even more challenging. Another security threat is the customer frequently changed data which is stored in the cloud like inserting, deleting, modifying, appending, re-ordering etc., [1]. Lastly deployment of cloud computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored

in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world.

In this paper, we focus on the Software as a service. In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its elasticity. This can be achieved by cloning tasks on to multiple virtual machines at run-time to meet the changing work demand. Load balancers distribute the work over the set of virtual machines. This process is not visible to the cloud user who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be more, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud based application software with a similar naming convention: communication as a service, test environment as a service, desktop as a service.

Several trends are opened up the era of cloud computing, which is an internet based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

The tremendous benefits, outsourcing computation to the commercial public cloud is also depriving customer's direct control over the systems that consume and produce their data during the computation, which brings in new security concerns and challenges towards this promising computing model. On the other hand, the outsourced computation on the cloud server often certain sensitive information, such as the government records, business records, research data and so on. [1].

To take action against the unauthorized information leakage, sensitive data have to be encrypted before outsourcing. So as to provide end-to-end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying plaintext data, making the computation over encrypted data a very hard problem [1]. On the other hand, the operational details which are done inside the cloud are not transparent to customers. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results that is they may behave beyond the classical semi honest model. For example, for the computations that require a large amount of computing resources, there are huge financial incentives for the cloud to be "lazy" if the customers cannot tell the correctness of the output. [1] Besides, possible software bugs, hardware failures or even outsider attacks might also affect the quality of the computed results. Thus, we can say that with respect to the customer's point of view the cloud is not secure.

II. RELATED WORK

Some recent results from the SujayP.Pawar and U.M.Patil et al. Secured Data Outsourcing in Cloud Computing [14] by someencryption and decryption techniques shows good results towards the data in a secured way in cloud. The cloud efficiency and communication latency is good at the level of the algorithms they used, but they did not specified the server side process.

Recently, Li and Atallah[9] had given a study for secure and collaborative computation of linear programming under the SMC framework. Their solution is based on the additive split of the constraint matrix between two involved parties, followed by a series of interactive cryptographic protocols collaboratively executed in each iteration step of the simplex algorithm. This solution has the computation asymmetry issue mentioned previously. Besides, they only consider honest-but-curious model and thus do not guarantee that final solution is optimal.

According to secure outsourcing of sequence comparisons, the author M.J.Atallah said that, we now more precisely stated that the edit distance problem, in which the cost of an insertion or deletion or substitution is a symbol-dependent non-negative weight, and the edited distance then the least-cost set of insertions, deletions and substitutions required to transform one string in to other. More formally, if we let λ be a string of length n, λ=λ1,..λn and μ be a string of length m, μ=μ1,…μm, both over some alphabet ∑. There are three types of allowed edit operations to be done on λ: insertion of a symbol, deletion of a symbol, and substitution of one symbol by other [5].Each operation has a cost associated with it, namely I(a) denotes the cost of inserting the symbol a, D(a) denotes the cost of deleting a, and S(a,b) denotes the cost of substituting a with b. Each sequence of operations that transforms λ into μ has a cost associated with it and least cost of such sequence is the edit-distance. The edit path is the actual sequence of operations that corresponds to the edit distance. According to secure outsourcing of scientific computation the authors M.J.Atallah et al said that [9], they produced the first investigation of secure outsourcing of numerical and scientific computation. A set of problem dependent techniques are proposed for different scientific applications like linear algebra, sorting, string pattern matching etc. However, these techniques explicitly allow information disclosure to certain degree. Atallah et al. discuss in the paper [10] and [11], produced two protocol designs for both secured sequence comparison outsourcing and secured algebraic computation outsourcing. However, both protocols used heavy cryptographic primitive such as homomorphic encryption or transfer and do not scale well for large problem set.

According to Non-interactive verifiable computing: Outsourcing computation to entrusted workers the author R.Gennaro [4] said that, the work is based on the crucial observation that Yao's Garbled Circuit construction, in addition to providing secure two-party computation, also provides a "one-time" verifiable computation. In other words, we can adapt Yao's construction to allow a client to outsource the computation of a function on a single input. More specifically, in the preprocessing stage the client grables the circuit C according to Yao's Construction. Then in the "input preparation" stage, the client reveals the random labels associated with the input bits of x in the garbling. This allows the worker to compute the random labels associated with the output bits, and from them the client will reconstruct F(x). If the output bit labels are sufficiently long and random, the worker would not be able to guess the labels for an incorrect output, and therefore the client is assured that F(x) is the correct output.

III. STATEMENT OF PROBLEM

Here we considered data storage architecture with two different things. Firstly, the cloud customer has large amount of data outsourced problems in to the cloud server. Second, the cloud servers, which have different data resources and provide different utility services, like hosting the public cloud in a pay-per-use manner. In this system, we focused on the data storage on the cloud. In the cloud, cloud customer / user can upload his/her data on the cloud server in the original format. So the data is not secure because the cloud sever is not fully honest model. It misbehaves with cloud customer and losses or corrupts the user's important data. So we have to

analyze this problem of data security and design some goal to achieve the data security problem on cloud.

IV. DESIGN GOALS

To enable secured data storage on the cloud, our system design should achieve the following security goals and performance of the system.

Input/output Secrecy – No sensitive information from the user's perspective the private data can be derived by the cloud server during the data storage

Correctness- Any cloud server that faithfully follows the mechanism must produce an output that can be decrypted and verified successfully by the customer.

Deliverance – No cloud server can generate an incorrect output that can be decrypted and verified successfully by the customer with zero error probability.

V. OBJECTIVES

Objective 1: Here we are mainly concentrating on the Secured Data Storage, which it will give a good assurance, faith to the cloud customer.

Objective 2: For providing security to the data, we are using the asymmetric encryption and decryption algorithms and check sum generation algorithms on both ends of Cloud Server and Cloud customer for more reliability to the user's data.

VI. SYSTEM MODEL

This system provides secured data storage in a cloud using encryption and decryption techniques. It provides efficient result verification. This method shows the overview of secured data storage and different techniques which it transforms the accessing operations on cloud (read, write, insert, delete, substitute etc,).

VII. DESIGN

Here, we have developed a system which it provide secured data storage in the cloud done by encryption and decryption techniques. The result verification is done at cloud server side. A secret key, Checksum, encryption and decryption steps done at the cloud client side. This includes the following steps.

Secret Key Generation – It is generated when the data is encrypted using RSA with size of 128-bit key length. This is key is generated only on the cloud customer side and it is saving on the customer's window. The key we used to decrypt the data is different because as we are using the asymmetric algorithm for providing security.

Checksum Generation – Before storing the data to cloud server, user generates a checksum value, for this generation we use SHA-2 cryptographic hash function and it will be given to cloud provider after encrypting with users private key. After receiving the document the cloud provider does the same thing Authorize Documents – cloud provider will digitally sign the user documents on request. This allows the user to use these electronic copies of the documents anywhere as and when necessary. For this the cloud provider provides the authentication by adding his digital signature to the document which can be verified by the public key he provided on request.

Result Verification – In this, we check the input given to server and output retrieved from the server. Here, we can compare the input and obtained output.

VIII. SECURITY MECHANISM

In the security mechanism, we give the best security to cloud customer for storing data on the cloud server and protect cloud customers data from losses and corrupt. So for providing better security to cloud, we check user authentication. The authentication is done through the cloud customer's login. So for user's login we apply the SHA2algorithm to encrypt the user authentication password which it is converted in 512-bit length.

Before uploading the data to cloud server, user

generates a checksum value and it will be given to cloud provider after encrypting with users private key. The data is stored on the server in unencrypted form means original data. Cloud provider stores the encrypted checksum and cloud customers public key. Then cloud provider generates the checksum value for that data and sends it to the cloud customer in encrypted format along with cloud provider's public key.

Whenever user wants to verify his data integrity, he will be provided with cloud provider's public key and encrypted checksum of the document. Then the encrypted data can be decrypted with public key of cloud provider and the customer can able to verify his data by comparing the decrypted checksum with the checksum which he generated before uploading the document to the cloud. This checksum verification mechanism gives more strength and security to the customer's data and proves the integrity of the data on cloud.

At the same time this also provides protection against no repudiation of either party. If the cloud customer denying something about his data, cloud provider can prove that his document is original by retrieving the encrypted checksum provided by the user at the time of uploading the data to cloud. Conversely if the cloud provider denying that the data uploaded by cloud customer was compromised it can be proved by providing the encrypted checksum given by the cloud provider at the time of document upload to the cloud customer.

IX. FLOW CHART

Secret Key generation, Input and Output Decryption can be done with the help of asymmetric algorithm named RSA algorithm. For this the flow chart is follows:

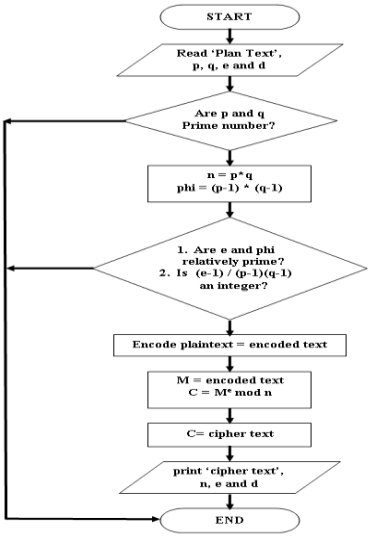

Fig 1Key pair generation using RSA

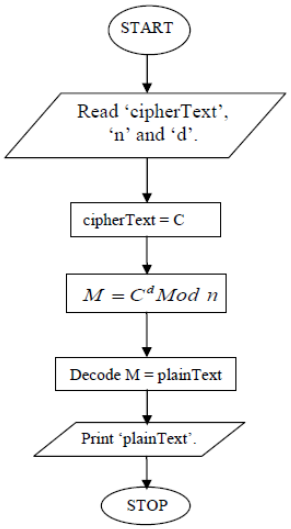

Figure 2. Decryption process of data

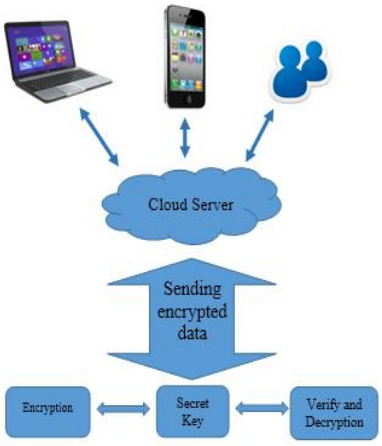

Figure 3. Secure Architecture

X. RESULTS

After finishing the implementation details, we have analysed the system performance and it is behaviours by giving different input sizes.

XI. SYSTEM REQUIREMENTS

We now assess the practical efficiency of the implemented system with experimental results. We have implemented "Security to the data in a cloud" using with some configuration. It includes both the customer and the cloud side processes in visual studio 2010 and SQL server R2 for storing database. Both customer and cloud server computations in our experiment are conducted on the same work station with an Intel Core i5 running at 2.0 GHz with 8GB RAM. Here, we also use the cloud environment, there we install all cloud resources and its environment on our system to use relative cloud environment. Here, we also calculated communication latency between the cloud server and cloud customers.

XII. IMPLEMENTATION

In this mechanism, we have implemented both the cloud server and cloud customer using algorithm steps. In the algorithm steps run on both cloud server and cloud customer side. In the given algorithm steps Secret key generation, Checksum Calculation, Input Encryption, Output Decryption, Result Verification at both sides of the cloud customer and server. Here, we checked the system performance with the text data as input value and we observe the system behavior by giving this text data as input in different sizes. We recorded time (sec) for this variable size data. As shown in fig.2 we calculated the cloud efficiency for the variable input data and fig.3 shows the communication latency of cloud customer with cloud server.

The efficiency of cloud increases with increase in data sizes up to certain limit and then it will decreases. We calculated the communication latency, which is also increase as the input data size increased.

XIII. CONCLUSION

As the Cloud computing use the internet for sharing the resources so the security of the data is the main issue in the cloud. So in this paper, we formalize the problem of secured storage of data in cloud. Here, we provide the input/output privacy and correctness / soundness guarantee. So the customer's data will be secure on the cloud server and customer data will be secure on the cloud and the personal data may not be corrupted by the server. Here, we also checked the communication latency of the cloud to notice the performance of the system.

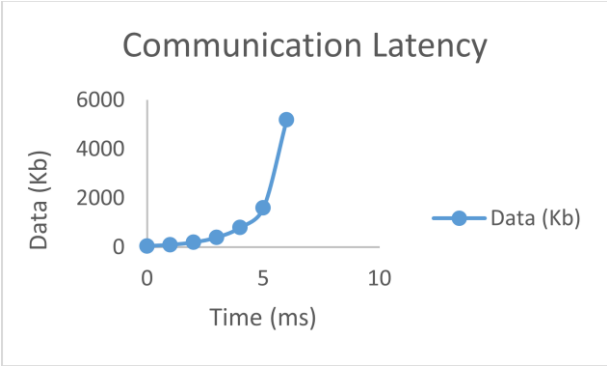

Figure 5. Communication Latency Graph

Figure 4. Cloud Efficiency Graph

XIV. ACKNOWLEDGEMENT

At the time of making the data, collection on this area many people were helped me a lot. I specially thank Dr. R.SivaRamaPrasad for his valuable guidance on this area and my sincere thanks to my family and friends.

XV.REFERENCES

[1] C.Wang.K.Ren and J.Wang, "Secure and practical outsourcing of linear programming in cloud computing", IEEE Transaction on cloud computing. Pp.820-828, 2011.

[2] C.Wang.Q.Wang.K.Ren and W.Lou, "Ensuring data storage security in cloud computing" in Proc.of IWQoS'09,July 2009

[3] S.Hohenberger and A.Lysyanskaya, "How to securely outsource cryptographic computations", in Proc.of TCC, 2005, pp 264-282

[4] R.Gennaro, C.Gentry and B.Parno, "Non-Interactive verifiable computing : outsourcing computation in entrusted workers" in Proc. of Cryto'10,Aug 2010.

[5] M.Atallah and K.Frikken, "Securely outsourcing linear algebra computations" in Proc.of ASIACCS, 2010. pp 48-59

[6] N.Gohring, "Amazon's S3 down for several hours", "amazonwebservices (AWS)"

[7] Sun Micro Systems Inc, "Building customer trust in cloud computing with transparent security" 2009.

[8] M.J.AtallahK.N.Pantazopoulos, J.R.Riece and E.H Spafford, "Secure outsourcing of scientific computations", advances in computers,vol.54, pp 216-272,2001.

[9] M.J.Atallah and J.Li."Secure outsourcing of sequence comparisons" int. J.inf.sec.vol.4.no4.pp 277-287,2005

[10] D.Benjamin and M.J.Atallah "Private and cheating free outsourcing of algebraic computations" in proc.of 6th conference on privacy security and trust (pst),2008,pp 240-245

[11] A C C Yao, "Protocols for secure computations" in proc of FOCS'82 1982 pp 160-164.

[12] O.Goldreich, S.Micali and A.Wigderson "How to play any mental game or a completeness theorem for protocols with honest majority" in proc. of STOC'87 1987,pp 218- 229.

[13] W.Du and M.J.Atallah, "secure multi-party computation problems and their applications: a review and open problems" , in proc.of New security paradigms workshop (NSPW), 2001 pp.13-22

[14] SujayP.Pawar and U.M.Patil"Secure Data Outsourcing in Cloud" in ICACCE'2014 29-33.