International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Securing Data in Cloud Environments by Using RSA Algorithm

Namita Jhende[1] and Raghvendra Kumar[2]
[1,2]Dept. of Computer Science & Engineering, LNCT Group of College, Jabalpur, MP, India
jhendenamita@gmail.com, raghvendraagrawal7@gmail.com

Abstract

Cloud computing is an innovative computational manner for satisfying the need of new generation computing and the storage solutions. That offers scalable computing performance as well as storage solution therefore more than one cloud service providers are collaborating together for offering the scalable solutions. Additionally the data outsourcing techniques are developed to reduce the overhead of maintenance and reducing the computational cost. But data hosting on third party servers is always un-trusted. Therefore keep preserve the data on third party servers in secure manner need a cryptographic solution for data storage. One of the principal challenges of resource sharing on data communication on the cloud network is its security. This is premised on the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical. This paper presents a design of data encryption and decryption in a cloud environment using RSA algorithm with a specific message block size. The RSA algorithm allows a message sender side to generate a public keys to encrypt the message and the receiver side is sent a generated private key using a secured database on the cloud. An incorrect private key will still decrypt the encrypted text message but to a form different from the original text message.

Keywords: *Cloud Computing, Privacy Preservation, Data Storage, Java Servlet and Microsoft Azure.*

1. Introduction

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no

longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially form id able task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third-party auditing process should bring in no new vulnerabilities towards user data privacy. With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results.

Cloud storage system enables storing of data in the cloud server efficiently and makes the user to work with the data without any trouble of the resources. In the existing system, the data are stored in the cloud using dynamic data operation with computation which makes the user need to make a copy for further updating and verification of the data loss. An efficient distributed storage auditing mechanism is planned which overcomes the limitations in handling the data loss.

The many advantages of cloud computing are increasingly attracting individuals and organizations to outsource their data from local to remote cloud servers. In addition to cloud infrastructure and platform providers, such as Amazon, Google, and Microsoft, more and more cloud application providers

are emerging which are dedicated to offering more accessible and user friendly data storage services to cloud customers. Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system.

Cryptography is playing a major role in data protection in applications running in a cloud computing environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day-to-day life because many people interact electronically every day; through e-mail, e-commerce, ATM machines, smart phones, etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users. Despite the fact that secured communication has existed for centuries, the key management problem has prevented it from commonplace application. The development of public-key cryptography has enabled large-scale network of users that can communicate securely with one another even if they had never communicated before.

2. Literature Survey

Mobile hand held device such as smart phones has increasingly became powerful in years. Smart phones are not only with voice oriented device but also equipped with wide capabilities with internet access. With the advent of cloud services for mobile application, it has greatly enhanced the scalability and security. As mobile devices become more like PC's, it tends to carry and store all kinds of data such as check books, cameras, planners, mp3 players, etc., in cloud that can be accomplished for Google Android phones. The primary objective of "cloud based mobile data storage system" is to create a full-fledged Android app.

Cloud computing is the delivery of computing as a service rather than a product. It provides shared resources, software, and information to computers and other devices over a network. 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 centres. We can store and retrieve the data as we like using cloud computing. With the increasing popularity of cloud computing, huge amount of documents are outsourced to the cloud for reduced management cost and ease of access. Although encryption helps protecting user data confidentiality, it leaves the well-functioning yet practically-efficient secure search functions over encrypted data a challenging problem

Dongyoung Koo et al [1] proposed an efficient data retrieval scheme using attribute-based encryption. The proposed scheme is best suited for cloud storage systems with massive amount of data. It provides rich expressiveness as regards access control and fast searches with simple comparisons of searching entities. The proposed scheme also guarantees data security and user privacy during the data retrieval process.

Cong Wang et al [2] utilize and uniquely combine the public key based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, author further explore the technique of bilinear aggregate signature to extend the main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

Ning Cao et al [3] define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE).

Author establishes a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, they choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. In further use "inner product similarity" to quantitatively evaluate such similarity measure. First propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

C. Selvakumar et al [4] introducing a partitioning method for the data storage which avoids the local copy at the user side by using partitioning method. This method ensures high cloud storage integrity, enhanced error localization and easy identification of misbehaving server. To achieve this, remote data integrity checking concept is used to enhance the performance of cloud storage. In nature the data are dynamic in cloud; hence this work aims to store the data in reduced space with less time and computational cost.

W. Sharon Inbarani et al [5] proposed a threshold proxy re-encryption scheme and integrate it with decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the

storage servers to another user without retrieving the data back.

Emiliano Miluzzo et al [6] provided invest significant effort into designing, building, and empowering cloud infrastructures. At the same time, technological advances are commoditizing small devices with powerful compute, storage, and communication capabilities at unprecedented scale. What if such devices could extend the boundaries of the traditional cloud model to form an even more flexible, resource-aware, and better-performing cloud?

Kalyani Bangale et al [7] present a method to secure data collection server by protecting and developing backups used for Health Care Cloud. The Objective of Smart Remote Health Care Data Collection Server (SRHDCS) is to provide Auto Response Server, Better Solutions for Data Backup and Restore using Cloud, Availability of data remotely using safer protected data transmission and Confidentiality of data remain intake. The Smart Remote Health Care Data Collection Server can collect data and send to a centralized repository in a platform independent format without any network consideration. The central repository is also a source for other vendors/depts. to use the information for their specific requirement. The purpose of Smart Remote Health Care Data Collection Server is to help users (basically admin) to collect information from any remote location even if network connectivity is not available at that point of time.

V. Malligai et al [8] can stored all kind of mobile data in cloud and access simultaneously. The user can retrieve all the data in mobile itself and can also access this data through web. Thus it reduces the overhead of using only mobile to get back the data which serves the purpose of making our data secure and flexible (i.e) to be available anywhere.

P. Srinivas et al [9] proposed ineffective and flexible distributed scheme with Token Generation algorithm for data files checking as a secure and dependable cloud storage service. A new scheme was introduced to encrypt with the user specified key parameters to make the resource more robust. They derive a new algorithm which is very light weight and easy to compute. Here stores the encrypted blocks into cloud and perform token checking on this encrypted blocks which gives more security to data. Author verifies the data effectively in case of any block modifications of files before storing to Clouds by token acknowledgment. The proposed scheme is highly efficient and resilient against attacks like Byzantine server failures, malicious data modification attack. Two way verification of file blocks which results more robust and ensure that data will not be modified before reaching to clouds.

Wenhai Sun et al [10] presented a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, they propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. To improve the search efficiency, we propose tree-based index structure and various adaption methods for multi-dimensional (MD) algorithms so that the practical search efficiency is much better than that of linear search. To further enhance the search privacy, author propose two secure index schemes to meet the stringent privacy requirements under strong threat models, i.e., known cipher text mode land known background model. Finally, they demonstrate the effectiveness and efficiency of the proposed schemes through extensive experimental evaluation.

3. Proposed Work

This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder therefore protecting unauthorized person from having access to the data even if they are able to break into the system. There are many ways of classifying data cryptographic algorithms but for the purpose of this paper, they will be classified based on the number of keys that are employed for encryption and decryption. The three common types of algorithms are:

a. Private Key Cryptography: The Private key uses only a single key for both encryption and decryption. The schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing while block cipher scheme encrypts one block of data at a time using the same key on each block.
b. Public Key Cryptography: Public key uses one key for encryption and a different key for decryption. Modern PKC was first described using a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a private key [5]. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. RSA is one of the first and still most common PKC implementation that is in use for key exchange or digital signatures.

3.1 The Design of the Java programming

An object programming language (of which java is one of them) uses a unified form of describing each programming steps and also called Unified Modeling Language (UML). It is a standard notation that originated in the mid-1990s from the work of James Rumbaugh, Ivar Jacobson and Grady Boch. This language is more secure on the internet and provide. This language is platform independent and highly secure. It is a graphical way of representing and designing an object oriented language for proper description of each step involved and the flow layout of the program itself. This work chooses to use UML because it has the

advantage of clearly showing the relationship that exists between the classes, servlet that form this work. There are three packages that exist in this work, they are:

i. The application GUI Package
ii. The Microsoft Azure db interface Package

In this paper the Top-down approach is used for the design of the program therefore all the small objects are put together to form the main object. The individual classes and jsp file of these smaller objects are specified with names and are then linked together to form the major object. The class names for the individual objects are;

i. login.java
ii. session.java
iii. Test.java

The necessary java packages were imported while the database was created in Microsoft Azure that is provide huge data store facility. Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser and Back side refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage facility, create virtual machines, security mechanism, services, deployment models, servers, etc.

4. Results and Discussion

Virtual Private Cloud (VPC) services released by Google cloud, Microsoft Azure and Amazon are examples of Hybrid Cloud. From the service type's view, Cloud Computing can be classified as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). SaaS provide services to end users, while IaaS and PaaS provide services to ISV and developers - leaving a margin for 3rd party application developers this web service was authenticated user firstly then its sent login detail in the user registered mail id, then it was run and compiled on windows 8 or support any operating system and tested on Microsoft Azure. The Graphic User Interface (GUI) is designed to be user friendly and can be used without knowledge of programming in Java,jsp, servlet and cloud computing.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Figure 1

Figure 2

Figure 1: User Login Page in Cloud

Figure:2 User login by registered mail Id and perform Encryption and decryption Environment

The sender sent a test message "hello how is you?" The Plaintext ("hello how are you") is text file before clicking on encode to convert the text to Binary code (decrypted file) and the result is placed in the Encoded Text as shown in Figure 3

Figure 3: Here user select text file to perform Encryption

Figure 4: Encrypted text file is here

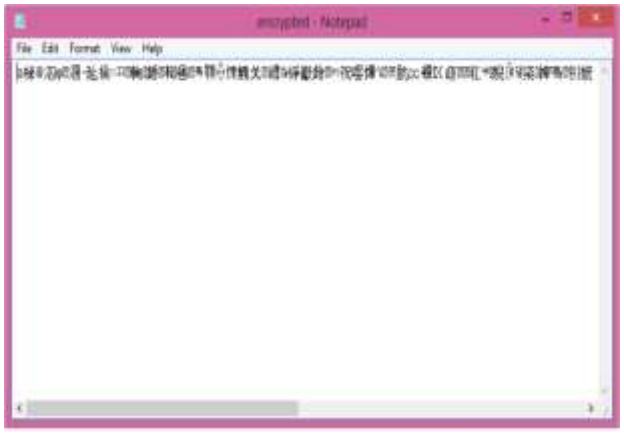
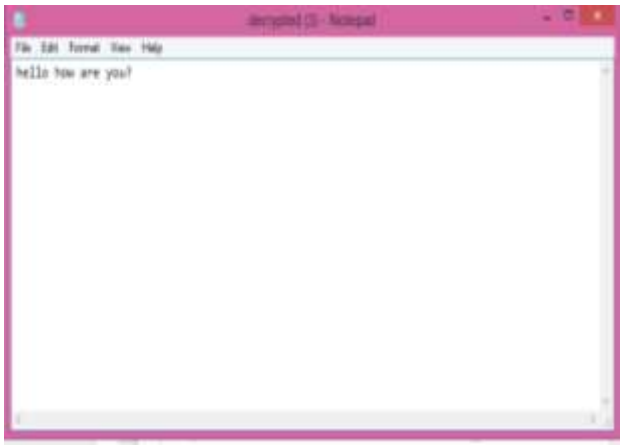


Figure 5. Decrypted text file is Here At the receiver end, the

Figure 6 Now user select decryption for encrypted file



Bearing all security concerns in mind, authors have opted a hybrid structure of RSA Algorithm as solution to overcome the risk of Privacy and Confidentiality, integrity, security, Storage, Backup and Recovery. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only. In this paper author perform security on text file using RSA Algorithm .and futures we will perform security of any file with highly secure.

5. Conclusion

This paper successfully integrated on premise and Cloud-deployed SaaS software using Web Services. The Cloud vendor provided infrastructure services were used to address scalability, performance, security, availability, disaster recovery, monitoring requirements of the system. With this web

services, data can be transferred from one computer to another via an unsecured cloud environment. An eavesdropper that breaks into the message will return a meaningless text message. Obviously encryption and decryption is one of the best ways of hiding the meanings of a message from intruders in a cloud environment. This suggests that using of this technology can not only decrease our cost of implementation but also help us for saving a huge amount and proves a basics to utilize the minimum resources in a best way but with in a limited premises.

.

References

1. Dongyoung Koo, Junbeom Hur, Hyunsoo Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage", Computers and Electrical Engineering, 2012 Elsevier Ltd.
2. Cong Wang, Qian Wang, and Kui Ren,Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing",978-1-4244-5837-0/10/$26.00 ©2010 IEEE
3. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014
4. C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha, "PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique", 978-1-4673-4529-3/12/$31.00 c 2012 IEEE
5. W. Sharon Inbarani, G. Shenbaga Moorthy, C. Kumar Charlie Paul, "An Approach for Storage Security in Cloud Computing- A Survey",International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 1, January 2013
6. Emiliano Miluzzo, "I'm Cloud 2.0, and I'm Not Just a Data Center",10897801/14/$31.0 0 © 2014 IEEE Published by the IEEE Computer Society
7. Kalyani Bangale, Karishma Nadhe, Nivedita Gupta, Swati Singh Parihar, Gunjan Mankar, "Smart Remote Health Care Data Collection Server", International Journal of Computer Science and Mobile Computing, Vol. 3,

Issue. 2, February 2014, pg.415 – 422

8. V.Malligai, V. Venkatesa Kumar, "Cloud Based Mobile Data Storage Application System", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)© 2014, IJARCST All Rights Reserved 126Vol. 2 Issue Special 1 Jan-March 2014
9. P. Srinivas, K. Rajesh Kumar, "Secure Data transfer in Cloud Storage Systems using Dynamic Tokens", International Journal of Research in Computer and Communication technology, IJRCT, ISN 278-5841,Vol 2, Isue 1, January ,2013.
10. Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou,Hui Li, "Privacy-preserving Multi-keyword Text Search in the Cloud Supporting Similarity based Ranking", ASIA CCS'13, May 8–10, 2013, Hangzhou, China. Copyright 2013 ACM 978-1-4503-1767-2/13/05.