Secure Performance Analysis over Cloud

Shaikh Zaki Mohammed [1], Siddique Sadab Jahan [2], Singh Deepika [3], Ahlam Shakeel Ahmed Ansari [4]
Mohammed Haji Saboo Siddik College Of Engineering

Abstract

Cloud computing is today’s most frequent research area due to its ability to reduce cost associated with computing, increase in the efficiency, high availability and storing of mass data.

Along with such advantages cloud have some issues associated with security and advanced feature of data management. As the data is stored publicly on the cloud, this may leads to the leakage of data. So the information can be misused. Information retrieval has also become tedious because of large amount of data stored on the cloud.

In order to provide ease of access in accessing of data, we can use efficient data mining algorithm. We can also enhance the security measures by using encryption algorithm in order to prevent from unauthorized access. Encryption algorithm provide secure channel for data transmission. Hence the resulting system is protected and provides easily accessible data over cloud.

1. Introduction

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage.

The uniqueness of the Cloud Computing is that its ability to reduce the costs associated with computing, providing dynamic resource pools, increases the efficiency of computing and high availability. But there are some drawbacks such as privacy, security is very important aspects.

As data mining and security are the demand of the cloud computing environment; we use Apriori algorithm and RSA algorithm for generating the progress reports from the cloud storage and to guarantee the data storage security over cloud respectively.

In this paper, we proposed a system architecture that can be used by any organization for securing and mining their data over the cloud and that will provide them secure progress report for their performance analysis.

2. Cloud computing

Cloud Computing[1][2][3] is internet based computing, whereby shared resources, software and information are provided to computers and other devices on demand.

2.1. Cloud Computing Models

Cloud Providers offer services that can be grouped into three categories.

2.1.1. Software as a Service (SaaS). In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2.1.2. Platform as a Service (Paas). Here, a layer of software or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS examples.

2.1.3. Infrastructure as a Service (Iaas). IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

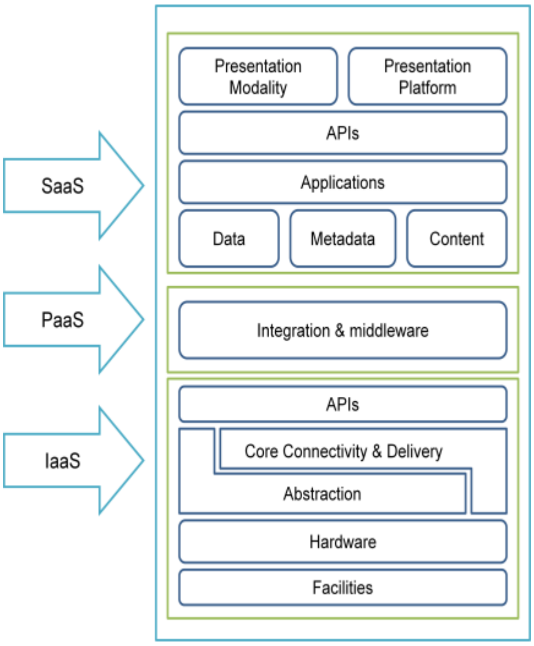

Figure 1: Cloud computing services

Our proposed system is mainly dependent on the SaaS model where the complete application has been provided to the end user. After login as a valid user into the system, the end user fires the query as per his requirement and after servicing that query the SaaS model generate the performance analysis report for the particular user.

3. Data security issues in the cloud

3.1. Data Location and Relocation

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location. Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others’ resources.

3.2. Privacy and Confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

3.3. Data Integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place For compliance purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed.

4. Data security

Data confidentiality and audit ability topped the list of primary obstacles for the use of cloud computing technologies in any organizations, according to a recent survey of over 1100 Indian Business Technology professionals.

When data mobility is at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework. High levels of data relocation have negative implications for data security[4][5][6] and data protection as well as data availability.

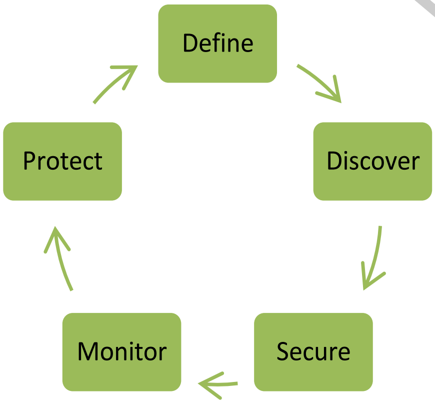

Figure 2: Data Security Cycle

5. RSA Algorithm

RSA[6][7] is the most popular a block cipher and asymmetric key cryptographic algorithm, in which every message is mapped to an integer. RSA used for providing secrecy, authentication and secure connection between nodes. 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.
RSA Algorithm consists of Three Steps:

- Key Generation
- Encryption
- Decryption

I. Key Generation

Before the data is encrypted, Key generation should be done.
Steps for key generation:

i. Choose two large prime numbers p and q .
ii. Calculate n = p * q.
iii. Compute Euler's totient function, Ø(n) = (p-1) * (q-1).
iv. Select the random encryption key which should be within the range 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1.
v. Compute d (decryption key) where d * e = 1 mod Ø(n). The range of d is 0<=d<=n.
vi. Publish the public key i.e. KU={e,n}
vii. Private key i.e. KR={d,p,q}.

II. Encryption

Encryption is the process of converting original plain text into cipher text.

Steps for encryption:

i. Cloud service provider should give or transmit the Public Key {e,n} to the user who want to store the data with him or her.

ii. Compute cipher text C is C = m^e(mod n).

III. Decryption

Decryption is the process of converting the cipher text into the original plain text.

Steps for decryption:

i. The cloud user requests the Cloud service provider for the data.

ii. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e., C.

iii. The Cloud user then decrypts the data by computing, m= C^d(mod n).

6. Data Mining

The data mining is a concept useful for retrieving required and desired data from data warehouse or a data base. User of the data base wants data for different purpose and for such purpose they fire different queries for it, only the desired data is retrieved from the data base. This process is done by efficient data mining algorithm. As there are lots of mining algorithm out of them one is Apriori algorithm.

In our proposed system, the Cloud storage contains the large set of data. At a time we require only some specific type of interrelated data. To reduce the complexity of searching the information into the large set of data we came to the idea of using data mining.

6.1. Apriori Algorithm

In this proposed system we have decided to use Apriori Algorithm because, it is the basic and popular data mining algorithm that able to find relations between data items stored in the data base. It provides item sets or data sets that occur most frequently together. This item sets can range from individual item to large set of items. It also includesassociation rule mining concepts that are based on strong rules present between different data items.

7. Proposed Solution

The proposed system consists of the[8] different levels of users i.e.; Top level, middle level and low level. They make use f login forms to interact with the system. They all are having the different roles in the system. Different levels of users are associated with different login name and password and according to their level of login they can access the system and do their work done.

The functional blocks are explained as follows:

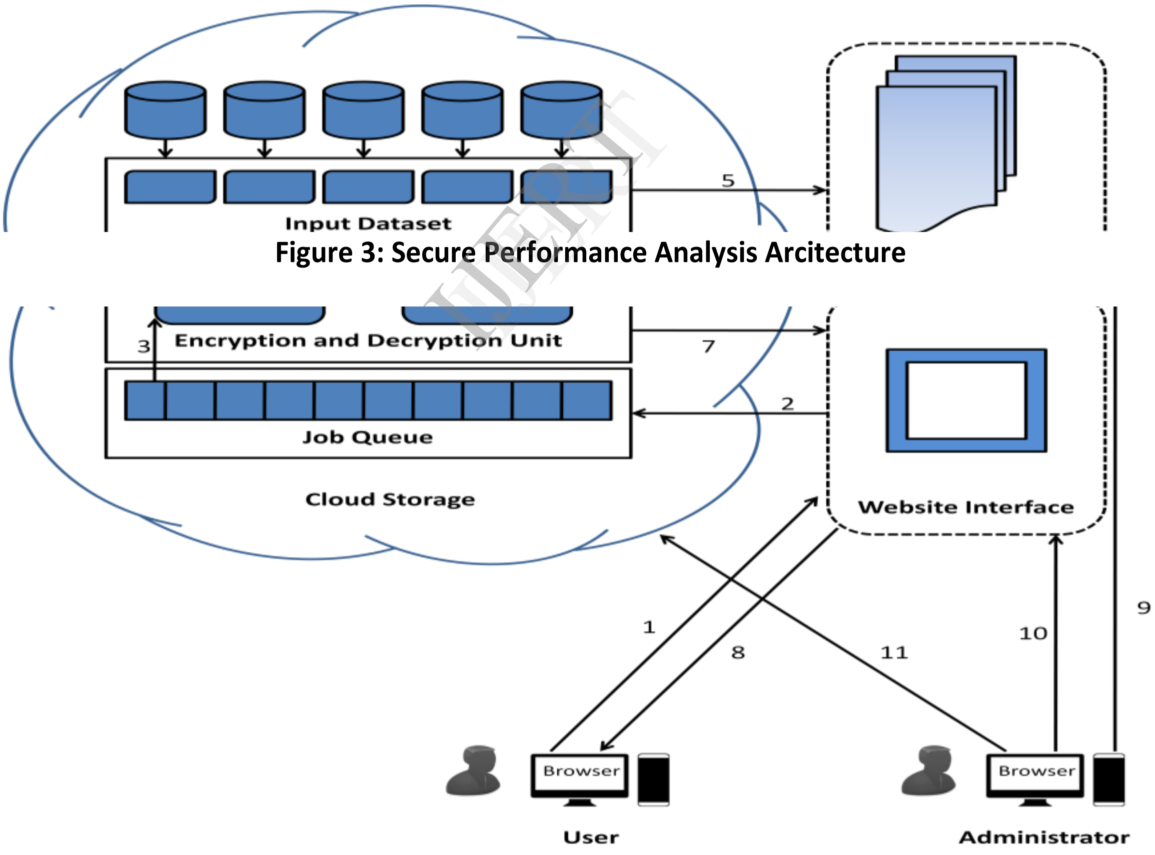

Figure 3: Secure Performance Analysis Arcitecture

1. Users

a) Student(Low level User)

The student is the person belonging to the organization that needs to enter his data into the cloud storage, wants to keep his data secure and to have full access over his own data.

b) Staff(Middle level User)

The Staff is a person belonging to the organization who needs to do some mining on the cloud storage that is related to his business but he requires the report and his request to be secret.

c) Administrator(Top level User)

The Administrator is a person belonging to the organization who needs to keep track over the entire data stored in the cloud.

2. Report Generator

Report generator generates report as per the request made by the users. It actually does the job of computations.

3. Cloud Storage

The storage is nothing but the collection of data where the entire data of each student is stored. The Storage unit has the sub-functional units that are as follows:

a) Input Datasets
b) Encryption Decryption Unit
c) Job Queue

4. Web Browser

The browser is responsible to submit the users request in an encrypted format to the website and receive the secure forecasting report and provide it to the end user.[8]

5. Website Interface

It is Web server instance that caters the request of the user and forwards it to the task queue and receives the resultant report and replies back to the user.[8]

The following steps are performed to extract a report from the Cloud Storage (see Figure 3):

1. User interacts with the Website interface through the browser that encrypts the request using RSA algorithm as shown in Figure. 3
2. Website interface put this job request into the job queue.
3. The requested job is decrypted by the encryption and decryption unit as shown in Figure. 4.
4. The encryption and decryption unit sends the decrypted request to the report generator for further processing.
5. The different datasets are extracted then forwarded to the report generator.
6. The report generator generates the report and sends the report to the encryption unit.
7. The encryption unit generates an encrypted report using the same RSA algorithm and sends it to the website interface.

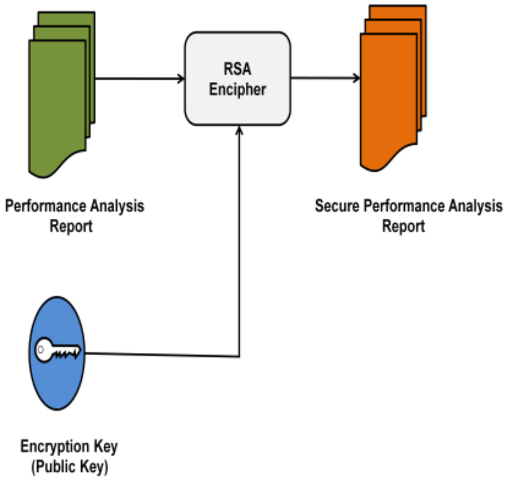
RSA Encipher
Performance Analysis Report
Secure Performance Analysis Report
Encryption Key (Public Key)

Figure 4: Encryption unit

8. The browser then decrypt received report using the RSA algorithm.

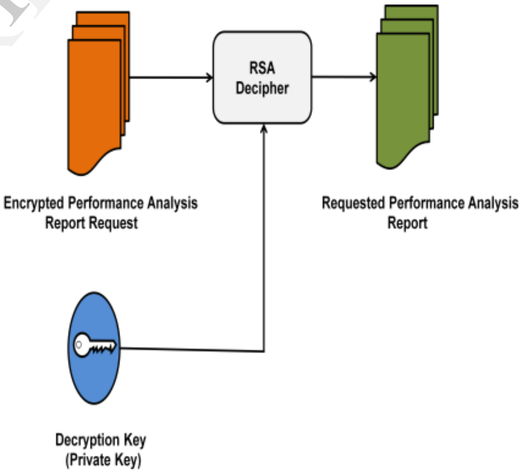
RSA Decipher
Encrypted Performance Analysis Report Request
Requested Performance Analysis Report
Decryption Key (Private Key)

Figure 5: Decryption Unit

9. Administrator can manage the report generator system in order to work as per expected.
10. Administrator keeps the website interface updated.
11. Administrator keep track on the cloud storage in order to maintain such a huge amount of data accurately.

8. Application

By taking an example we can clearly understand the working of the system and its each and every component. There is a College which provide degree of many courses. The college have to keep track on the student's progress reports for every year of all the subjects. And the information needs to be retrieved for some other analysis. For example, student enters marks of their own and professors need to retrieve the marks of students for some computations and calculations.

So to accomplish this task the user (professor) does the following steps:

1. The user access the web site using their own browser, they fire some query. Their query is encrypted before sending it to the web site using a key.
2. The encrypted query received by the web site interface and then this request is placed in job queue.
3. From the job queue the encryption decryption unit selects this particular request then decrypt it.
4. This decrypted query is then given to Report generator. It simply solves the query and the result will be generated in the form of reports.
5. This report is encrypted in the encryption unit using the key.
6. The encrypted report is send back to the user through the web site interface.
7. The web browser decrypts the report using the key.

9. Acknowledgement

We are thankful to Mohammed Haji Saboo Siddik College of Engineering, for providing us the opportunity to do constructive work. We also thank anonymous reviewers for their constructive suggestions.

10. References

[1] Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom*, "Cloud Computing Security: From Single to Multi-Clouds", La Trobe University, Bundoora 3086, Australia, 2012

[2]Kashif Munir and Prof Dr. Sellapan Palaniappan, "FRAMEWORK FOR SECURE CLOUD COMPUTING", 2School of Science and Engineering, Malaysia University of Science and Technology, Selangor, Malaysia

[3] Pankaj Arora*, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja, " Cloud Computing Security Issues in Infrastructure as a Service", *Punjab Technical univ.*

[4] Eman M.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", The 8th International Conference on INFOrmatics and Systems (INFOS2012), 14-16 May.

[5] Nir Kshetri, "Privacy And Security Issues In Cloud Computing", The University of North Carolina-Greensboro, USA

[6] Vijeyta Devi & Vadlamani Nagalakshmi, "A Prospective Approach On Security With Rsa Algorithm And Cloud Sql In Cloud Computing", Department of Computer

science, GITAM University, Andra Pardesh, India, May 2013.

[7]P. Syam Kumar* and R. Subramanian, “RSA-based dynamic public audit service for integrity verification of data storage in cloud computing using Sobol sequence”, School of Engineering and Technology, Pondicherry University, Puducherry-605 014, India.

[8] Ahlam Shakeel Ahmed Ansari & Kailas Kisan Devadkar, “Secure Cloud Mining”, Sardar Patel Institute of Technology Mumbai, India.