ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A New Approach for Data Security in Cloud Computing

Reeshma K, Anjali S, Thota Subhashini

Assistant Professor, Dept of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

Assistant Professor, Dept of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

M.Tech II Year Scholar (CNE), The Oxford College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Our financial resources are finite, but our computational needs are infinite. The demand for computational recourses keeps on increasing indefinitely, whatever the availability of resources, the need for 'more 'remains. Here the cloud plays its role, Cloud computing gets its name as a metaphor for the internet .Typically, the internet is represented in the network diagram as a cloud. The cloud icon represents "all that other stuff "that makes the network work. Many organizations are slowly shifting towards the use of Cloud computing, because Cloud computing promises to cut operational and capital cost and more importantly let IT departments focus on strategic projects instead of keeping the datacenter running. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers may be untrusted.To ensure the security and correctness of user's data in the cloud, this paper proposes a new paradigm for data Security in cloud computing.

KEYWORDS: Cloud, Security, Encryption, Decryption.

I. INTRODUCTION

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud was inspired by the symbol that's often used to represent the Internet in flowcharts and diagrams. Cloud computing is a general term for the delivery of hosted services over the Internet. Cloud computing enables companies to consume compute resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house.

Cloud computing promises several attractive benefits for businesses and end users. Three of the main benefits of cloud computing includes:

- Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.
- Elasticity: Companies can scale up as computing needs increase and then scale down again as demand decrease
- Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

Cloud computing services can be private, public or hybrid. Private cloud services are delivered from a business' data center to internal users. This model offers versatility and convenience, while preserving management, control and security. In the public cloud model, a third-party provider delivers the cloud service over the Internet. Public cloud services are sold on-demand, typically by the minute or the hour. Customers only pay for the CPU cycles, storage or bandwidth they consume. Leading public cloud providers include Amazon Web Services (AWS), Microsoft Azure, IBM/Soft Layer and Google Compute Engine. Hybrid cloud is a combination of public cloud services and on-premises private cloud – with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud while using the public cloud for bursty workloads that must scale on-

DOI: 10.15680/ijircce.2015.0306029

demand. The goal of hybrid cloud is to create a unified, automated, scalable environment which takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

Although cloud computing has changed over time, it has always been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as service (SaaS). IaaS providers such as AWS supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large, and memory- or compute-optimized instances, in addition to customized instances, for various workload needs. In the PaaS model, providers host development tools on their infrastructures. Users access those tools over the Internet using APIs, Web portals or gateway software. PaaS is used for general software development and many PaaS providers will host the software after it's developed. Common PaaS providers include Salesforce.com's Force.com, Amazon Elastic Beanstalk and Google App Engine. SaaS is a distribution model that delivers software applications over the Internet; these are often called Web services. Microsoft Office 365 is a SaaS offering for productivity software and email services. Users can access SaaS applications and services from any location using a computer or mobile device that has Internet access.

Cloud computing is suffering from several issues and one of the most significant is security, availability, privacy confidentiality, authentication, integrity and compliance. Security is most prominent issue in cloud computing and data security is top most challenge. Service provider might be honest but internal threat also a problem. Any insider malicious user can harm critical data such as medical and financial record. So tackle the data security issue we provide a new encryption scheme.

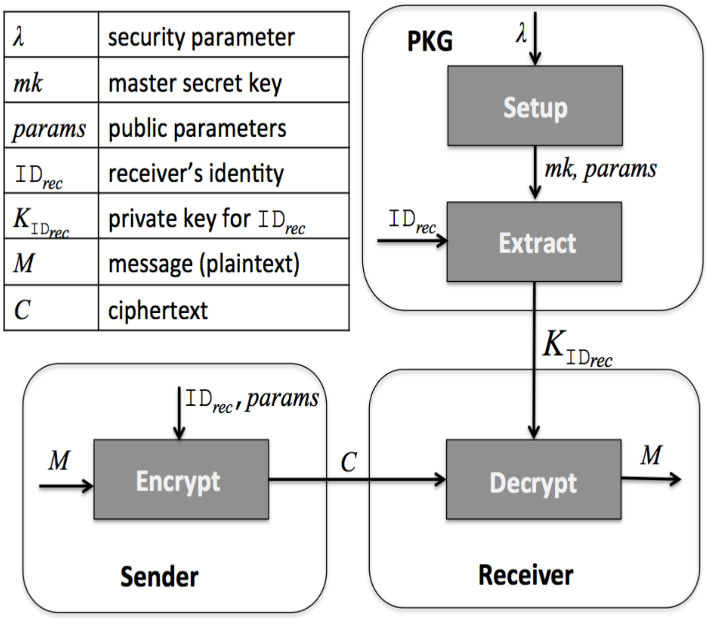
To summarize, our contributions in this paper are twofold:

- We introduce frame work: a cloud computing based model for large amount data information management in cloud datacenters, which provides not only flexibility and scalability but also security features.
- We present a security solution for the proposed model based on identity-based encryption schemes, which provides secure communication. The rest of this paper is organized as follows. In Section 2, we review the related work. Through Section 3 and 4 we present the proposed model and the security solution. This Section focuses on the general architecture of the frame work. Section 5 present experimental results and we conclude the paper in Section 6.

II. RELATED WORK

Two very basic cryptographic building blocks for the security are identity-based encryption (IBE) and identity-based signature (IBS) schemes. Introduced by Shamir in 1984 [43], identity-based cryptography is to eliminate the requirement of checking the validity of certificates in traditional public key infrastructure (PKI). In an identity-based encryption (IBE) scheme, the Private Key Generator (PKG), a trusted party, first generates secret master key mk and public parameter ϕ. Note that ϕ, which is long-term, will be given to every party that is involved. Once a receiver submits his/her identity, denoted by IDrec, the PKG computes the private key KIDrec associated with IDrec by running the private key extraction algorithm Extract providing its master secret key mk as input. Here, the identity IDrec can be any string such as an email address, a telephone number, etc. Note that the distribution of the private keys can be done in a similar way as digital certificates are issued in normal public key cryptography: Users would authenticate themselves to the PKG and obtain private keys associated with their identities. Secure channel may have to be established between the PKG and the users depending on the situation to prevent eavesdropping.

Now any sender, who is in the possession of IDrec, encrypts a plaintext message M into a cipher text C by running the Encrypt algorithm. Upon receiving C, the receiver decrypts it by running the Decrypt algorithm providing the private key KIDrec obtained from the PKG previously as input. The basic operations of the IBE scheme are illustrated in Figure 1.



λ	security parameter
mk	master secret key
$params$	public parameters
ID_{rec}	receiver's identity
$K_{\mathrm{ID}_{rec}}$	private key for ID_{rec}
M	message (plaintext)
C	ciphertext

Figure 1. Overview of identity-based encryption

III. PROPOSED MODEL

In this paper we are putting forward a new idea for data security in cloud computing. Our basic idea is to build the model at three hierarchical levels: top, regional and client levels in which the first two levels consist of cloud computing centers while the last level contains end-user smart devices. The top cloud computing center takes responsibility of managing general devices and accumulation of data across the regional cloud computing centers which are placed in the lower level in the hierarchy. The regional cloud computing centers are in turn in charge of managing intelligent devices, which have lower hierarchical level than the regional cloud computing centers in specific regions (e.g., within a city), and processing data of these devices.

The overall architecture is shown in Figure 2.

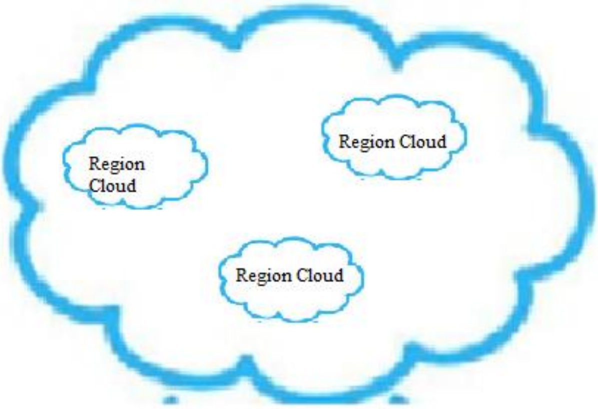


Fig.2 Top Cloud

The main idea of our security solution model is to allow all the involved entities, i.e., top and regional cloud computing centers and clients to be represented by their identities which can be used as encryption keys or signature verification keys. The entities in the lower level can use the identities of higher-level entities to encrypt their data for secure communication with the entities in the higher level. For example, the regional centers use the top cloud's entity to encrypt their messages. By employing an identity-based encryption scheme, the information storages, which are components of regional clouds, can encrypt the received confidential data from the end-user devices so that services requested by the end-users decrypt and process the confidential data without compromising the information storages' private keys. One of the obvious benefits we can gain from applying identity-based cryptography is that, they are using identities rather than digital certificates which depend on traditional PKI (Public Key Infrastructure), we can save significant amount of resources for computation and communications and resolve scalability issues. The saving gained from the elimination of digital certificate in the big data environment is especially momentous.

IV. SECURITY SOLUTION

In this architecture, a smart grid can be divided into several regions each of which is managed by a cloud computing center that can be setup from either a public cloud or a private cloud. The role of a regional cloud computing center is to manage intelligent devices in the region as well as to provide an initial processing for information received from these devices. Besides regional cloud computing centers, there is a special cloud computing center at the top level, which is in charge of managing and processing data for the whole cloud. Proposed Architecture is shown in Figure 3.

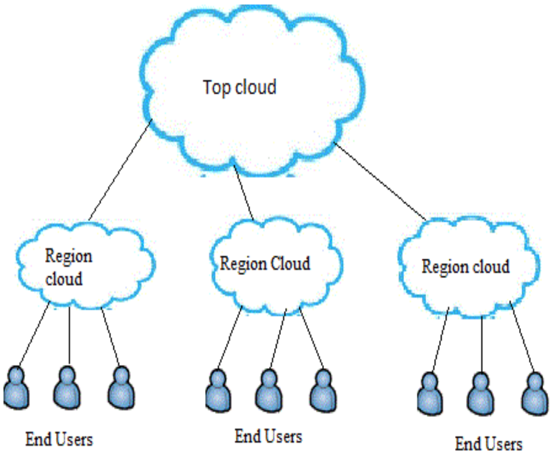


Figure 3: Proposed Architecture

In realizing the security framework, we make the following assumptions:

- There is a Private Key Generator (PKG) that can issue private keys for top and regional clouds, and clients when they register. We assume that the PKG is a party that has responsibility and capacity of maintaining the Smart-Frame usually at the national level and its credential is fully trusted.
- The top cloud, regional clouds and clients are identified by unique strings, which are to be used as encryption keys or signature verification keys.
- Each entity will obtain a private key associated with its identity, so it can decrypt the confidential data.
- Each entity will send confidential data to the entity which is only one-level higher. That is, the end-users send confidential data to the entities in the regional cloud only. Similarly entities in the regional cloud can send confidential data to the top cloud only.
- Each entity will authenticate data using the private key obtained from the PKG.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Based on the above assumptions, our main idea can be described as the following scenario, which is also depicted in Figure 3. At the top of the hierarchy is the top cloud, which consists of distribution services or management services. Below the top cloud, there are regional clouds that consist of general user services and information storages. These regional clouds, in turn, have higher hierarchy than smart (intelligent) end-user devices (simply we call “clients”), which are at the bottom of the hierarchy. Based on the principle of identity-based cryptography, the PKG will generate private keys for top cloud and any entities in regional clouds and end-users. Using their identifiers and private keys, each entity can utilize IBE schemes to secure information flow.

4.1 Data encryption

Data encryption is used to encrypt data before it is sent through the network. In general, before sending the data, the sender uses the identity of the target receiver as the key to encrypt the data.

- Upon receiving a Top cloud’s identity, the PKG generates a private key Pv3 associated with Top cloud by running the private key extraction algorithm Extract providing pv3 as input.
- Upon receiving a regional cloud’s identity, the PKG generates a private key Pv2 associated with Regional cloud by running the private key extraction algorithm Extract providing pv2 as input.
- Upon receiving a client’s identity, the PKG generates a private key Pv1 associated with client by running the private key extraction algorithm Extract providing pv1 as input.

Whenever a client has some data to store in cloud, which is highly confidential. At first the date is encrypted with public key of client (pb1) E (F, pb1), now the encrypted message (F’) is passed to regional cloud. At regional cloud center the encrypted data (F’) is encrypted by regional cloud public key (pb2) E (F’, pb2), after that the message (F’’) is send to top cloud. At top cloud center the message is encrypted again by Top clouds public key (pb3), E (F’’, pb3), finally the message (F’’’) is stored in Cloud service providers place for storage.

4.2 Data Decryption

Whenever a client is to retrieve his details it should travel all the way back, firstly the data stored in cloud storage providers place will be send to top cloud, here the data will be decrypted with top clouds private key (pv3) D (F’’’, pv3), the decrypted message (F’’) will be forwarded to regional cloud, at regional cloud place again it will be decrypted with private key (pv2) of regional cloud D (F’’, pv2). After that the message (F’) will be send to clients so that the client can easily decrypt the received message using its private key (pv1), so he will be getting the original message back.

```
Algorithm1: Message storage
Top: pv3, pb3
Regional: pv2, pb2
Client: pv1, pb1
Client → Regional
Client: F’=E (F, pb1)
Regional → Top
Regional: F’’=E (F’, pb2)
Top → CSP
Top: F’’’=E (F’’, pb3)
CSP: Store (F’’’)
```

```
Algorithm: Message Retrieval
Client → Regional: Request (F)
Regional → Top: Request (F’’)
Top → CSP: Request (F’’’)
CSP → Top: Send (F’’’)
Top: F’’=D (F’’’, pv3)
Top → Regional: Send (F’’)
Regional: F’=D (F’’,pv2)
Regional → Client: Send(F’)
Client: F=D (F’, pv1)
```

Here the algorithms involved in the proposed scheme are shown; Algorithm 1 shows the setup phase which includes the operations from starting to the storing data on the cloud. Algorithm 2 shows the file retrieval process which shows how the requested file by owner is transferred to him from cloud service provider.

V. EXPERIMENTAL RESULT

An application has been designed and implemented in java language on the network to achieve the functionalities of the client, regional cloud and top cloud. We have assumed that the end user, regional cloud and top cloud are in the same system domain and sharing the uniform system parameters. Through this application the messages can be transferred between these entities and the required result has been achieved.

VI. CONCLUSION

This paper has proposed a new approach to provide security and confidentiality to the data. The proposed model contains three pairs of encryption decryption processes to secure the data in such a way that no leakage of data on cloud will be happened. In this scheme encryption is used to provide security to the data while in transmit. Because the encrypted file is stored on the cloud, so user can believe that his data is secure. In this scheme only encrypted file is transferred over the channel, which reduces the problem of information disclosure.

REFERENCES

[1] Preeti Garg and Dr Vineet Sharma. An Efficient and secure data storage in mobile Cloud Computing through RSA and hash function.IEEE conference 2014

[2] Chien - An Chen,Myounggyu Won ,Radu Stoleru. Energy Efficient Fault-Tolerant Data Storage and Processing in Mobile Cloud.Volume 3 IEEE transactions on Cloud Computing.

[3] Fawaz S,Al-Anzi,Ayed A Salman,Noby K Jacob ,and Jyoti Soni. Towards, Robust, Scalable and Secure Network Storage in Cloud Computing.IEEE Conference 2014.

[4] Joonsang Baek, Quang Hieu Vu. A Secure Cloud Computing based framework for big data information management of smart grid. IEEE transaction on Cloud computing.

[5] Sushil Kumar Sah and Prof. Dr.Shashidhar Ram Joshi Scalabilty of Efficient and Dynamic Workload Distribution in Autonomic Cloud Computing. IEEE conference 2014.

[6] Chun-Wei Tsai, Wei-Cheng Huang, Meng-Hsiu Chiang, Ming-Chao chiang, and Chu-Sing Yang. A hyper-Heuristic Scheduling Algorithm for Cloud. IEEE Transaction on Cloud Computing 2014.

[7] Michael Armbrust, Armando Fox, Rean Griffith. A View of Cloud Computing. Communications of the ACM April 2010.

BIOGRAPHY

K Reeshma has done her B.Tech in Computer Science and Engineering from College of Engineering Vadakara Affiliated to Cochin University of science and Technology and M.Tech in Computer Science and Engineering from AMC College of Engineering Affiliated to Visvesvaraya Technological University. She has worked at MES Engineering College for three year. She is currently working as the **Assistant Professor** in ISE Department of The Oxford College Of Engineering since 2 years. She has guided many M.Tech students in Computer Network Engineering. She has over all 5 years of teaching experience.

Anjali S has done her B.Tech in Computer Science and Engineering from College of Engineering Adoor Affiliated to Cochin University of science and Technology and M.Tech in Computer Science and Engineering from AMC College of Engineering Affiliated to Visvesvaraya Technological University. She has 1.7 year industrial experience in Isigma Inc company. She is currently working as an **Assistance Professor** in ISE Department of The Oxford College Of Engineering since 1.5 years.

Mrs. Thota Subhashini a Student of Information Science and Engineering Department at The Oxford College of Engineering-Bangalore, affiliated to VTU pursuing **M.Tech** in Computer Networking and Engineering. She received her Bachelors of Engineering in Computer science and Information Technology Engineering from Nagarjuna Institute of Technology-Vijayawada affiliated to JNTU. She is currently working as a research assistant under the guidance of Assistant Prof. K Reeshma. Her research interests are Mobile Ad hoc Networks and Cloud Computing.

DOI: 10.15680/ijircce.2015.0306029