IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Cost Adequate Reliable and Anonymous Data Distribution with forth Security

G. Chandrika[1], N. Praveen Kumar[2], V. Sangeeta[3]

M.Tech Final Year, CSE, DIET, Anakapalle, India[1]

Asst. Prof, CSE, DIET, Anakapalle, India[2]

Head of the Department, CSE, DIET, Anakapalle, India[3]

Abstract: The popularity and widespread use of cloud have brought great convenience for data sharing and collection. Not only can individuals acquire useful data more easily, sharing data with others can provide a number of benefits to our society. Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing, there are several security goals a practical system must meet. By providing security of data in a cloud we can convert data into unknown format and stored into cloud. In this paper we are proposed mainly three concepts for performing authentication of data consumers, generation of group key and provide security of sharing data in cloud. By performing authentication of data consumers we can implement the concepts for identity based digital signature. By using this concept we can verify users are authenticated or not. After completion of authentication process the cloud will generate group key and send to all group members. By using that secret key each data consumer will retrieve data from the cloud and get original plain format. Before getting original plain format data each users will perform the decryption process. In this paper we are using blowfish encryption and decryption algorithm for converting data into unknown format and get original data by using decryption process. So that by implementing those concepts we can provide more security of data and also provide efficient user authentication.

Keywords: Cloud Computing, Security, Encryption, Decryption, Authentication.

I. INTRODUCTION

A Cloud computing is a technology which uses internet and remote servers to store data and application. In cloud there is no need to install particular hardware, software on user machine, so user can get the required infrastructure on his machine in cheap charges/rates [7]. Cloud computing is an infrastructure which provides useful, on demand network services to use various resources with less effort. Features of Cloud computing are, huge access of data, application, resources and hardware without installation of any software, user can access the data from any machine or anywhere in the world, business can get resource in one place, that's means cloud computing provides scalability in on demand services to the business users.

Everyone kept their data in cloud, as everyone kept their data in cloud so it becomes public so security issue increases towards private data. Data usage in cloud is very large by users and businesses, so data security in cloud is very important issue to solve. Many users want to do business of his data through cloud, but users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data [1], [2].Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service oriented cloud computing model. A health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only [3].

To solve the security issues in cloud; other user can't read the respective users data without having access. Data owner should not bother about his data, and should not get fear about damage of his data by hacker; there is need of security mechanism which will track usage of data in the cloud. Accountability is necessary for monitoring data usage, in this all actions of users like sending of file are cryptographically linked to the server, that performs them and server maintain secured record of all the actions of past and server can use the past records to know the correctness of action. It also provides reliable information about usage of data and it observes all the records, so it helps in make trust, relationship and reputation.

So account ability is for verification of authentication and authorization. It is powerful tool to check the authorization

DOI10.17148/IJARCCE.2016.51072

policies [4]. Accountability describes authorization requirement for data usage policies. The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. A study by Gartner considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations.

Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing.

Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers. In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide. Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [9]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing.

Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form. Security controls in Cloud Computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid.

Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data center's network under their control. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization are secure and they can meet their service-level agreements, and that they can prove compliance to auditors.

We present here a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment. A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats [5]. Here, we present a list of vulnerabilities and threats, and we also indicate what cloud service models can be affected by them. Furthermore, we describe the relationship between these vulnerabilities and threats; how these vulnerabilities can be exploited in order to perform an attack, and also present some countermeasures related to these threats which try to solve or improve the identified problems.

II. EXISTING SYSTEM

Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, including:

Data Authenticity: In the situation of Smart Grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency.

Anonymity: Energy usage data contains vast information of consumers, from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such applications, and any failures to do so may lead to the reluctance from the consumers to share data with others.

DOI10.17148/IJARCCE.2016.51072

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Efficiency: The number of users in a data sharing system could be HUGE (imagine a smart grid with a country size), and a practical system must reduce the computation and communication cost as much as possible. Otherwise it would lead to a waste of energy, which contradicts the goal of Smart Grid.

III. PROPOSED SYSTEM

Cloud computing is internet-based computing which contains large groups of remote servers that are interconnected to allow the centralized data storage as well as online access to various services or resources[8]. Popularity of cloud computing is increasing rapidly in distributed computing environment. In this paper we are implementing cloud architecture contains mainly three concepts for authentication of data consumers in cloud, sharing of secret key in a group members and also contain concepts for provide privacy of sharing data [6].

Cloud provides three service models, which are; platform as a service, infrastructure as a service and software as a service. Under the Database as a service, this is having four parts which are as per mentioned below.

- Encryption and Decryption - For security purpose of data stored in cloud, encryption seems to be perfect security solution.
- Key Management - If encryption is necessary to store data in the cloud, encryption keys can't be store there, so user requires key management.
- Authentication - For accessing stored data in cloud by authorized users.
- Authorization – Rights given to user as well as cloud provider.

To solve the security issues in cloud; other user can't read the respective users data without having access. Data owner should not bother about his data, and should not get fear about damage of his data by hacker; there is need of security mechanism which will track usage of data in the cloud. So that before store data into cloud the data owner will encrypt data using blowfish algorithm and stored into cloud. The data consumer will retrieve data from the cloud and decrypt using blowfish algorithm. Before performing encryption and decryption process each users will verify by cloud service for the purpose of authentication. In this paper we are using identity based digital signature schema for authentication of users. The implementation procedure of identity based digital signature schema is as follows.

1. Set up:
For each user, there is a secret key x which is selected by the signer, and public keys α, β, p_i
where: $\beta = \alpha^x \bmod p_i$

The public keys α, β, p_i are published in a public file and is known to everybody while the secret
keyx is kept secret.

$\alpha^x = \beta \bmod p_i$
(α,β,p_i) - public key
$x(1<x<\phi(p))$ is the signer's private key.

The above things are performed once by the signer.
p is a large prime.

2. Signature Generation
Choose a random number k such that $0<k<p_i-1$ and $\gcd(k,p_i-1)=1$.
$\gamma=\alpha^k \bmod p_i$
Choose a random number k such that $0<t<p_i-1$ and $\gcd(t,p_i-1)=1$.
$\lambda=\alpha^t \bmod p_i$
16
$m=(x\,\gamma + k\,\lambda + t\,\delta) \bmod (p_i-1)$
Signature of user is (γ,λ,δ).

After generating signature of each user will send that signature to cloud service. The cloud service will retrieve signature and again will generate signature and verify both signatures. The verification process will be done by cloud service is as follows.

3. Signature Verification
$\alpha^m = \beta^\gamma \gamma^\lambda \lambda^\delta \bmod p_i$
Using this equation the receiver verifies the authenticity of the signature by computing both sides
of the equation.

4. Key Generation Process:
The cloud service will verify all users' authentication status and generate secret key for all users in a cloud. The cloud service will choose secret key and send that key all users in a secure manner.

In this paper the cloud service will send secret point to individual users and using that secret point each user will get original secret key. The generation of secret points is as follows.

$$K = \text{Radom(range)}$$
$$X_i = K/P_i$$
$$Y_i = K\%P_i$$
$$\text{Secret Point}_i=(X_i,Y_i)$$

After generating secret points the cloud server will send those points to individual users in cloud. Before sending points to users the cloud server will also send status to individual users and also send secret key to data owner.

Encryption of sharing data using blowfish algorithm:
In this module the data owner will perform the encryption process for converting data into unknown format and stored into cloud. Before performing encryption process the data owner will retrieve secret key from the cloud service and encrypt data using blowfish encryption process. After encrypting shred data the data owner will stored into cloud.

DOI10.17148/IJARCCE.2016.51072

Decryption of sharing data using blowfish algorithm:
In this module each user or data consumer will retrieve data from the cloud and perform the decryption process of blowfish algorithm. Before performing blowfish decryption process each user will retrieve authentication status and secret points from the cloud service. if the authentication status is true it will get secret points and generate secret key. The generation of secret key is as follows.

$$K = X_i * P_i + Y_i$$

After getting secret key each user will retrieve cipher format data from the cloud and decrypt that data. after completion of decryption process each user will get plain format data.

IV. IMPLEMENTATION

The below is the implementation of cost adequate reliable and anonymous data distribution with forth security.

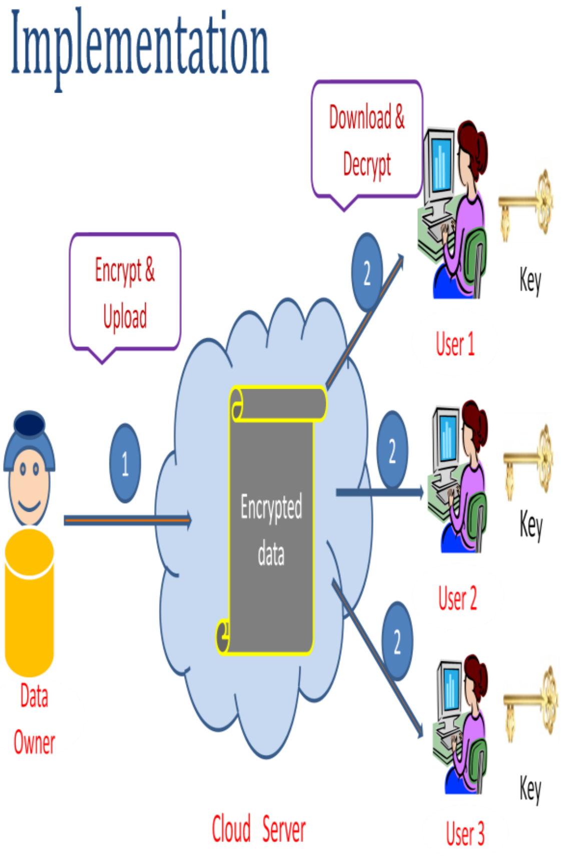
The popularity and widespread use of"CLOUD" have brought great convenience for data sharing and collection. Data acquiring process can also be more easy through sharing data with others can provide a number of benefits to our society compare to individual data processing. Data sharing is always deployed in a hostile environment and vulnerable to a number of security threats.

By using this "Cost Adequate Reliable and Anonymous Data Distribution with forth Security" concept we can verify users are authenticated or not. . Everyone kept their data in cloud, so it becomes public so security issue increases towards private data. By performing authentication of data consumers we can hide the data from third party users for providing identity based digital signature.

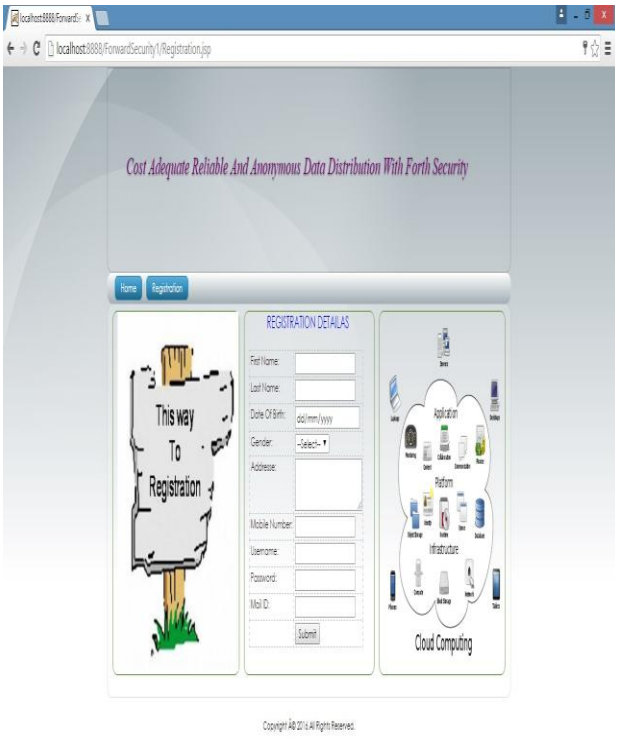
After transfer data from Owner to Users, they will receive secret key along with encrypted data, by using this key the data will decrypted. Cloud computing popularity is increasing rapidly in distributed computing environment.

In this paper we are implementing cloud architecture contains mainly three concepts for 'authentication of data consumers in cloud', 'sharing of secret key in a group members 'and also contain 'concepts for provide privacy of sharing data'.

- Encryption and Decryption –Protected data using digital signature along with secret key and decrypt shared data by using this secret key.
- Key Management – It maintains state conditions of secret key through entire data sharing process.
- Authentication - For accessing stored data in cloud by authorized users.
- Authorization – Rights given to user as well as cloud provider.



The entire process is described with screen shots of implementation.



Cost Adequate Reliable And Anonymous Data Distribution With Forth Security

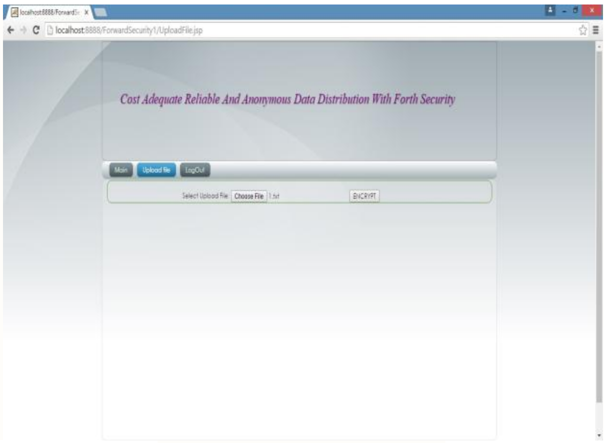
REGISTRATION DETAILAS

First Name:	
Last Name:	
Date Of Birth:	dd/mm/yyyy
Gender:	--Select--
Address:	
Mobile Number:	
Username:	
Password:	
Mail ID:	
	Submit

Copyright Â© 2016 All Rights Reserved.

1. Registration Form

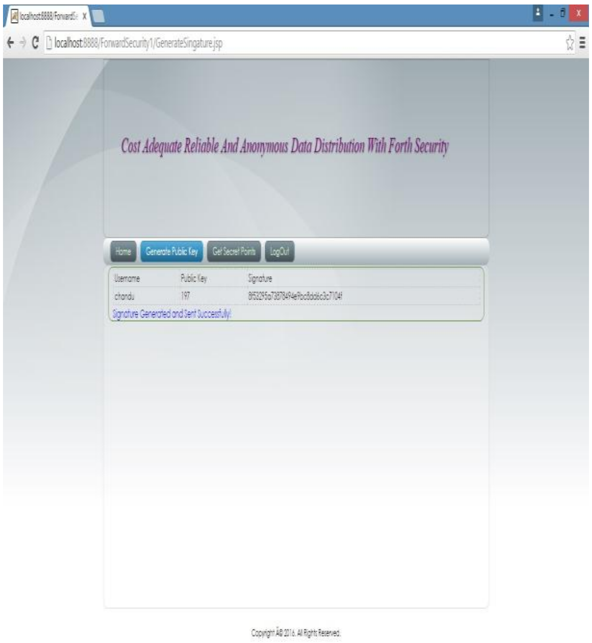
DOI10.17148/IJARCCE.2016.51072


localhost:8888/ForwardSecurity1/UploadFile.jsp

Cost Adequate Reliable And Anonymous Data Distribution With Forth Security

Select Upload File: Choose File 1.txt

2. Public Key Generation


localhost:8888/ForwardSecurity1/GenerateSingature.jsp

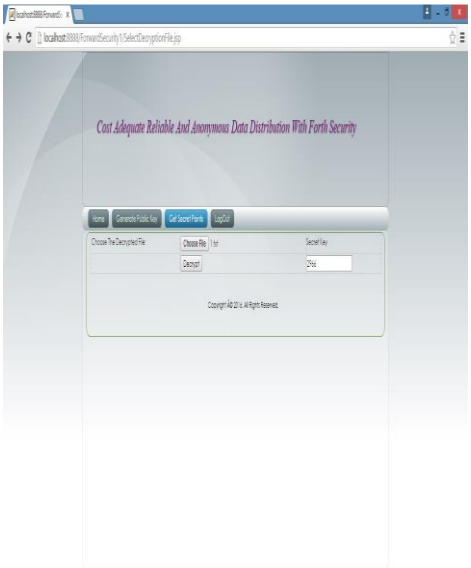
Cost Adequate Reliable And Anonymous Data Distribution With Forth Security

Username	Public Key	Signature
chandu	197	8f53295a73878494e9bc8dd6c3c7104f

Signature Generated and Sent Successfully!

Copyright Â© 2016. All Rights Reserved.

3. Encryption Form


localhost:8888/ForwardSecurity1/SelectDecryptionFile.jsp

Cost Adequate Reliable And Anonymous Data Distribution With Forth Security

Choose The Decrypted File: Choose File 1.txt

Secret Key: 29d

Copyright Â© 2016. All Rights Reserved.

4. Decryption Form

V. CONCLUSION

In this paper present an effect approach for performing authentication of data consumers and also provide more privacy of shared data in a cloud. Before performing sharing of data each user will verify by the cloud service for the purpose of authenticated user or not. After completion of authentication process the cloud service will send authentication status to individual users in cloud and also send secret key. Before sharing data in the cloud the data owner will stored data into cloud in the form of cipher format. So that by converting data into cipher format the data owner will user blowfish encryption process stored data into cloud. If any user will retrieve data from the cloud and decrypt that using blow fish algorithm will get original plain format data. By implementing those concepts we improve efficiency of authentication process and also provide more privacy of shared data in cloud.

REFERENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin,"Ensuring Distributed Accountability for Data Sharing in theCloud,", IEEE Transaction on dependable a secure computing,VOL. 9, NO. 4, pg 556-568, 2012.

[2] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang,"Promoting Distributed Accountability in the Cloud," Proc. IEEEInt'l Conf. Cloud Computing, 2011.

[3] ZhiguoWan, Jun'e Liu,Robert H. Deng, "HASBE: AHierarchical Attribute-Based Solution for flexible and ScalableAccess Control in Cloud Computing".

[4] HP Cloud website.

[5] S. Pearson , Y. Shen, and M. Mowbray," A privacy Managerfor Cloud Computing," Proc. Int'l Conf. Cloud Computing(cloudcom), pp.90-106,2009.

[6] S. Pearson and A. Charlesworth, "Accountability as a WayForward for Privacy Protection in the Cloud, " Proc First Int'l conf.Cloud Computing, 2009.

[7] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu,"A Logic for Auditing Accountability in Decentralized Systems,"Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security andTrust, pp. 187-201, 2005.

[8] A. Squicciarini , S. Sundareswaran and D. Lin, " PreventingInformation Leakage from Indexing in the Cloud," Proc. IEEEInt'l Conf. Cloud Computing, 2010.

[9] B. Chun and A. C. Bavier ,"Decentralized Trust Managementand Accountability in Federated System," Proc. Ann. Hawaii Int'lConf. System Science (HICSS), 2004.

[10] A. K. Awasthi and S. Lal. Id-based ring signature and proxyring signature schemes from bilinear pairings. CoRR,abs/cs/0504097,2005.

DOI10.17148/IJARCCE.2016.51072