Data Security Enhancement in Cloud Computing using Proxy Blind Signature

Subasish Mohapatra
Department of Computer Science and Application
College of Engineering and Technology Bhubaneswar, Odisha, India

Subhadarshini Mohanty
Department of Computer Science and Engineering
College of Engineering and Technology Bhubaneswar, Odisha, India

Arunima Hota
Department of Computer Science and Engineering
College of Engineering and Technology Bhubaneswar, Odisha, India

Shradha Pattanayak
Department of Computer Science and Engineering
College of Engineering and Technology Bhubaneswar, Odisha, India

ABSTRACT

Cloud computing is a rapidly growing internet based computing that endeavors to be dynamic, reliable and available with guaranteed quality of service. This has become a sophisticated computing platform or technology for customers as well as organizations for its availability of resources such as software, storage and network with minimum cost. Using the business model like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS) this environment have increased distribute computing capacity. Preserving confidentiality, integrity and availability are the vexing issues in cloud computing environment. This paper highlights cloud computing threats and proposes a distributed and efficient encryption algorithm to enhance the data security in cloud.

Keywords

Cloud Computing, Security threats, Proxy blind signature.

1. INTRODUCTION

Nowadays, cloud computing is one of the substantial technology. It is luring many companies and customers around the world due to its distributive architecture. It is a network based environment that allows sharing of computation as well as resources. Customers whether belongs to small or large organization are drawn toward cloud's promise of nimbleness reduced cost and enhanced IT resources [1]. IT companies are transforming their services from providing their own IT infrastructure to utilize computation services provided by cloud to their IT need [1]. Even cloud computing provides abundant opportunities to its customer but still it has lot of issues to be resolved. Security is one of the challenging issues in this computing paradigm .The virtual environment in the cloud system provide essential feature for scalability and availability .It has special security threats which are different from threats in physical system .In this paper a new approach has been considered for data security in cloud computing environment. The remaining sections are organized as follows: Section 2 presents cloud characteristics and their service models. Section 3 elaborates the cloud computing security threats. Data security responsibilities are explained in section 4.Proposed security model and the performance are described in Section 5 and Section 6 respectively. Finally the paper draws a conclusion and discusses future work in Section 7.

2. CLOUD FEATURES AND SERVICE MODELS

2.1 Cloud Computing Characteristic

This section discusses different essential characteristics of cloud environment defined by NIST (National Institute of Standard and Technology) [2]. Shared Resources: It is also known as Resource pooling. Resources are not used exclusively, rather than pooled together to serve multiple customers. This creates a sense of location independence where user is not aware of its computation being executed [3]. On Demand Service: Users can get service in plug and play fashion without intervention of human. This is also called as automatic computing in the fly. Elasticity: this characteristic allows customers or organizations to massively scale up the resources to business service. They can also de-allocate resources and return to pool after completion of task. Measured Services: Cloud users pay on computational basis. Cloud systems automatically controls and optimize resource use by leveraging and metering capability at some level of abstraction appropriate to the service [4]. Cost Reduction: Reduced cost due to computational efficiency and faster deployment of new business process.

2.2 Cloud Service Model

The services provided by cloud computing can be classified into three service models. This models are the basis of all services provided by cloud computing. Software as a Service (SaaS): In this service model software is provided by the vendor over internet in one too many forms. Instead of buying the software and installing it on their systems, users pay per use for subscription. Another advantage of this service is its centralized updating. So users must not worry for versioning [5]. Platform as a Service (PaaS): This model facilitates utilization of developing environment itself. User application always targets certain platform with tools provided by platform provider. Providers deploy and run this application on this platform with full control over application. Such application may require from third parties. Infrastructure as a Service (IaaS): users are allowed to access computing infrastructure itself. They can use computing power, storage medium and necessary networking components provided by vendors. Users can run arbitrary software and operating system that best meets their requirements with full control and management.

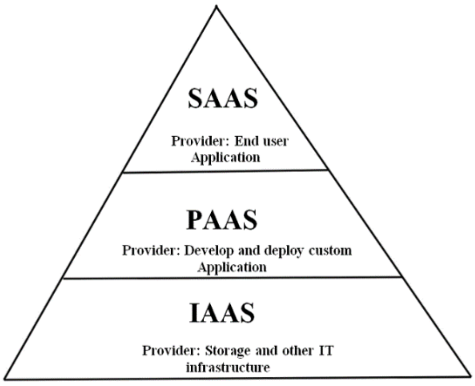
SAAS
Provider: End user Application
PAAS
Provider: Develop and deploy custom Application
IAAS
Provider: Storage and other IT infrastructure

Fig 1: Security in cloud service model.

2.3 Cloud Deployment Model

There are three types of cloud environments: public, private, hybrid and community cloud. Public Cloud: Public cloud is a standard model that provides application and storage for public. Multiple customers can share computing resources at same instance. Although it has compelling advantages, there exists hidden danger of security and quality of service. Private Cloud: Private cloud refers to internal services of an organization that is not available for ordinary people. Private cloud provides hosted services to particular group of people behind firewall. It is usually deployed in the enterprise's data center and managed by service provider. Hybrid Cloud: This is the combination of public as well as private cloud. In this model cloud provider has a service that has private cloud part which is only accessible by authorized access.

3. CLOUD COMPUTING SECURITY THREATS OR ISSUES

Cloud computing is the fastest growing segment in IT industry. Cloud services are altering the way enterprises build their infrastructure and applications. Cloud service delivery model creates cloud of virtual perimeters as well as a security model with responsibilities shared between customers and cloud service providers. This shared responsibility leads to many security challenges [6]. Attackers to the cloud system are broadly classified into two categories such as insiders and outsiders. Malicious employee at client, malicious employee at cloud and cloud provider itself are known as insiders. Generally, intruders are known as outsiders. Malicious Insiders: Malicious employee at client can learn the known as outsiders. Malicious Outsiders: Malicious employee at client can learn the password, authentication information, gain control over the virtual machines and access the information. Similarly, malicious employee at cloud can log into client communication and can read unencrypted data, monitor network communication and application partners etc. But cloud providers as intruders can read information about client data, behavior and violate confidentiality and integrity of data. Malicious Outsiders: Outsiders attack may be passive or active. In passive attack the objective of attacker is to obtain information. They do not modify data or harm to system. However, they may harm the sender or receiver message. In other hand active attack may change data and harm to the system. Malicious outsiders listen to network traffic, insert malicious traffic and probe cloud structure. Their goal is to break security in different aspects such as: data confidentiality, data integrity, access control and non repudiation [7]. Insecure Application Program Interface: Cloud service delivery model based on third party control. They have full control over application and configuration. Data location: cloud stores the data in distributive manner. It maintains transparency. When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage architecture can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud. Recovery: It is very difficult task to recover form failure if a cloud provider broke or the server fail. Furthermore, clients don't prefer to give permission to third-party companies to control their data. This issue can cause an impasse in security. Data Loss: By deleting without back up, loss of encoding key, unauthorized access usually put data in danger of being lost or stolen [8]. Some other security issues are related to failure in cloud provider's security, availability and reliability of internet, integrating providers and customer's security systems and legal and regulatory issues.

4. DATA SECURITY AND RESPONSIBILITY

In cloud environment data are stored in distributed manner. Users neither know the exact location of their data nor the other sources of data collectively stored in the pool. It is a challenging task to maintain confidentiality, integrity and availability of data in cloud platform. Measure security panorama in cloud computing is data privacy. While using public cloud, regardless of SaaS, PaaS, IaaS, it is important to ensure that the protocol must provide confidentiality as well as integrity. The confidentiality of data stored in public cloud has two potential concerns. First method is the access controls which consist of both authorization and authentication and the second one is the protection of data stored in cloud involves the use of encryptionData can be encrypted for confidentiality but can't satisfy integrity. Integrity also requires the usage of message authentication cede. Simplest way to use this method on encrypted data is to use a block symmetric algorithm in different mode. Cloud providers are responsible for managing all aspects of network, server, and application infrastructure. Since the application is delivered as a service to end users via web browser. Network based control are becoming less relevant and are superseded by user access controls [9]. Similarly, they are responsible for managing access control to the network, servers and application for PaaS delivery model [10]. In IaaS delivery model customers are entirely responsible for managing all aspects of access control their resources in cloud such as virtual servers, virtual network, virtual storage and application running on that infrastructure. Data in cloud server may be at rest or in transit state. Data at rest can be protected by using encryption. But limitation of this method in data rest will prevent indexing and searching. Organizations can encrypt data during transfer to or from a cloud provider and its data at rest might be encrypted using simple storage. But organizations data is not required for encryption if it is processed in cloud. For any application to process data, the data must be in unencrypted form [12]. In June 2009, IBM announced homomorphic encryption scheme which allow data to be processed without being decrypted. Although the homomorphic scheme has broken the theoretical barrier to fully homomorphic encryption, it requires immense computational effort. Different traditional cryptanalyst has developed several security models to mitigate the data security problems that exist in the cloud environment. The facilities given by cloud provider as well as user especially induce security problem in cloud environment [11].

The key solution for confidentiality and integrity is access control. This can prevent unauthorized user access to information system. This should cover different phases of authentication process like initial registration, registration for subscription as well as deregistration process. Another confidentiality consideration for encryption is the proper key management [13]. In the following section authors have proposed a security model to enhance cloud security.

5. PROPOSED SECURITY MODEL

This section explains an efficient DLP based proxy blind signature scheme for data security. The scheme is divided into five phases: system setup, proxy delegation, blind signing, signature extraction and signature verification.

5.1 Terminology for the algorithm

These are the following terminologies used in the algorithm as parameters and analysis.

- O the original signer.
- P the proxy signer.
- A, the signature asker.
- p, q two large prime numbers with q|(p-1).
- x_0 the original signer O's secret key.
- y_0 the original signer O's public key, $y_0 = g^{x0}$ mod p.
- x_p the proxy signer P's secret key.

5.2 Proxy Delegation Phase

Original singer O selects random number and computes R0 = gk0 (mod p) (1). s0 = x0 + k0. h (mw // R0) (mod q) (2). O sends (Ro, s0) along with the warrant mw to the proxy signer. And then proxy signer checks: gs0 = y0.$R_0^{h(m_w//R_0)}$ (mod p) (3). If it is correct, P accepts it a computes proxy signature secret key spr as follows: spr = so + xp(4). Responding proxy public key ypr = yo.yp$R_0^{h(m_w//R_0)}$= g^{spr} (modp).

5.2 Blind Signing Phase

Proxy signer P selects random number [*] and compute: r = gk (modp) (5) and then sends (Ro, r) to signature asker A. To obtain the blind signature of message m, original signer A randomly choose two random numbers u, v [*] and computes: r*=r.gu (yo.yp)-v (modp) (6). e*=h(r*//m) (modq) (7). e=e*-v(modq) (8). If r*= 0 then A has to select new tuple (u, v).

Otherwise A sends e to P. After receiving e proxy signer P computes: s*= k + espr(9) and sends the sign message s* to A.

5.3 Extraction Phase

While receiving s*, A computes: s = gs^{*+u}.$R_0^{-vh(m_w R_0)}$ (10).

Finally, the signature of message m is (m, mw, s, e*, R0).

5.4 Verification Phase

The recipient of signature can verify the proxy blind signature by checking whether e*=(h(sy_{pr}^{-e*}modp//m))(modq) (11) where ypr= yoyp$R_0^{h(m_w//R_0)}$. If it is true, the verifier accepts it as a valid proxy blind signature, otherwise rejects. The message flows of the proxy blind signature scheme are described in Figure 2.

5.6 Verifiability

This scheme satisfies the property of verifiability. The verifier can verify the proxy blind signature by checking

$e^* = \left(\mathrm{h}\left(\mathrm{s}.\, \mathrm{y}_{\mathrm{pr}}^{-e^*}\mathrm{modp}//\mathrm{m}\right)\right)$ (modq) holds this is because

.y modp

$\mathrm{g}^{s*+u}.\mathrm{R}_0^{-vh(m_w R_0)}\mathrm{y}_{\mathrm{pr}}^{-e*}\mathrm{modp}$

$\mathrm{g}^{k+e_{spr}+u}\mathrm{R}_0^{-vh(m_w//R_0)}\mathrm{y}_{\mathrm{pr}}^{-e*}\mathrm{modp}$

g^{k} +e*s$_{pr}$-vs$_{pr}$+u.$\mathrm{R}_0^{-vh(m_w//R_0)}\mathrm{y}_{\mathrm{pr}}^{-e*}\mathrm{modp}$

$\mathrm{g}^{k+e^*.s_{pr}+u}\mathrm{g}^{-v.x_0}\mathrm{g}^{-v.x_p}\mathrm{R}_0^{vh(m_w//R_0)}\mathrm{R}_0^{-vh(m_w//R_0)}\mathrm{y}_{\mathrm{pr}}^{-e^*}\mathrm{modp}$

$\mathrm{g}^{k+u}\mathrm{g}^{e^*}\mathrm{s}_{pr}$ ($\mathrm{g}^{x_0}\mathrm{g}^{x_p}$)-v$\mathrm{y}_{\mathrm{pr}}^{-e^*}$modp

$\mathrm{g}^{k+u}\mathrm{y}_{\mathrm{pr}}^{e^*}$($\mathrm{g}^{x_0}\mathrm{g}^{x_p}$)-v$\mathrm{y}_{\mathrm{pr}}^{-e^*}$modp

r$\mathrm{g}^{u}\left(\mathrm{y}_0\mathrm{y}_p\right)$-v modp

r^*

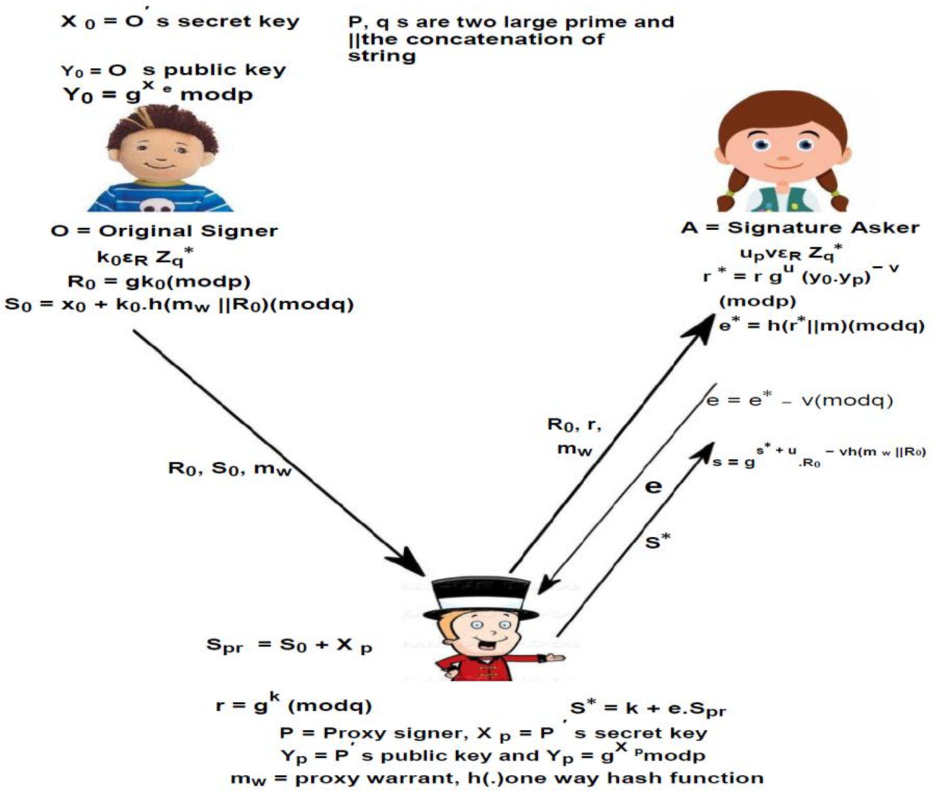
X 0 = O΄s secret key
P, q s are two large prime and ||the concatenation of string
Y0 = O s public key
Y0 = g^X e modp
O = Original Signer
k0εR Zq*
R0 = gk0(modp)
S0 = x0 + k0.h(mw ||R0)(modq)
A = Signature Asker
upvεR Zq*
r * = r g^u (y0.yp)^− v (modp)
e* = h(r*||m)(modq)
e = e* – v(modq)
s = g^s* + u.R0 − vh(m w ||R0)
R0, r, mw
R0, S0, mw
e
s*
Spr = S0 + X p
r = g^k (modq)
S* = k + e.Spr
P = Proxy signer, X p = P΄s secret key
Yp = P΄s public key and Yp = g^X pmodp
mw = proxy warrant, h(.)one way hash function

Fig 2: Prototype of the Proposed Model

6. PERFORMANCE EVALUATION

The performance of the proposed model in terms of number of keys, computational complexity has been analyzed in this section. Here the different key sizes in a private cloud network and their verification times are recorded and shown in the Table 1.

Table 1: Time Required For Overall Process (In Nano Seconds)

Description	Key Size	Proposed Model
Overall Process	4 bit	42630752
	8 bit	202244176
	16 bit	4521469262
	32 bit	8027003211
	64 bit	15076000875

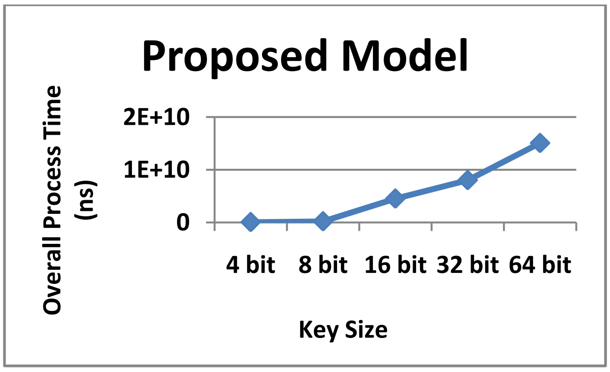

Fig 3: Completion time of the proposed model for different key sizes

7. CONCLUSION

Security is one of the promising issues in cloud computing environment. A proxy blind signature based data security mechanism to enhance the cloud security is proposed in this work .The data security in cloud computing environment is examined by varying different key size and obtained the overall processing time. The prototype model is tested in a private cloud environment. In future, this model can be tested in a real- time environment in public cloud. Efficiency of the system can be enhanced by providing more secure transaction. In data security, most foundations can be built upon confidentiality, integrity, and availability. This model can be a good idea in cloud world. In future, the researchers can enhance the work by developing more secure algorithms for better security and Quality of service.

8. REFERENCES

[1] Manvi, Sunilkumar S., and Gopal Krishna Shyam. "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey." Journal of Network and Computer Applications 41 (2014): 424-440.

[2] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[3] Nandgaonkar, Suruchee V., and A. B. Raut. "A comprehensive study on cloud computing." International Journal of Computer Science and Mobile Computing 3.4 (2014): 733-738.

[4] Stieninger, Mark, and Dietmar Nedbal. "Characteristics of cloud computing in the business context: A systematic literature review." Global Journal of Flexible Systems Management 15.1 (2014): 59-68.

[5] Yau, Stephen S., and Ho G. An. "Software engineering meets services and cloud computing." Computer 44.10 (2011): 47-53.

[6] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." Information Sciences 305 (2015): 357-383.

[7] [7] Ajoudanian, Sh, and M. R. Ahmadi. "A novel data security model for cloud computing." International Journal of Engineering and Technology 4.3 (2012): 326.

[8] Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6.1 (2014): 25.

[9] Liu, Bingwei, et al. "Information fusion in a cloud computing era: a systems-level perspective." IEEE Aerospace and Electronic Systems Magazine 29.10 (2014): 16-24.

[10] Priyadharshini, V., and A. Malathi. "Survey on software testing techniques in cloud computing." CoRR, abs/1402.1925 (2014).

[11] Wei, Lifei, et al. "Security and privacy for storage and computation in cloud computing." Information Sciences 258 (2014): 371-386.

[12] J. Katz, A. Sahai, and B. Waters, "Predicate Encryption, Supporting Disjunctions, Polynomial Equations, and InnerProducts," LNCS vol. 4965/2008, pp. 146-162, ©Springer Berlin Heidelberg, 2008.

[13] Sahu, Rajeev Anand, and Sahadeo Padhye. "Provable secure identity based multi- proxy signature scheme." International Journal of Communication Systems 28.3 (2015):497-512.