International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

An Advanced Implementation for Cryptography and Encryption in Cloud Computing Using Identity Based Encryption Techniques

Indra Kishor[1]

Assistant Professor, Department of CSE Arya Institute of Engineering and Technology, Delhi Road Kukas, Jaipur, Rajasthan, India
ijs2k8[at]gmail.com

Abstract: ***Cloud computing provides clients with a virtual computing infrastructure on top of which they can store data and run applications. While the benefits of cloud computing are clear, it introduces new security challenges since cloud operators are expected to manipulate client data without necessarily being fully trusted. We are designing cryptographic primitives and protocols tailored to the setting of cloud computing, attempting to strike a balance between security, efficiency and functionality. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers which is not within the same trusted domain as data owners. To keep sensitive user data confidential against un trusted servers, cryptographic methods are used by disclosing data decryption keys only to authorized users. This paper explores various data encryption techniques such as homophormic encryption, searchable and structured encryption, Identity based encryption, signature based encryption etc.***

Keywords: Computing, Encryption, Cryptography, Cloud Computing Security

1. Introduction

Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to computers on a pay-as-you-use basis. Users can access these services available on the "internet cloud" without having any previous knowledge on managing the resources involved. Thus, users can concentrate more on the core business processes rather than spending time on gaining knowledge on resources needed to manage their business processes.

2. Cloud Computing Architecture

Cloud computing architecture is divided into two sections: **the front end** and the **back end**. They connect to each other through a network usually called the Internet. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. On the back end of the system are the various computers, servers and the data storage systems that create the cloud of the computing services. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other.

3. Types of Clouds

Cloud providers typically center on one type of cloud functionality provisioning: infrastructure, Platform of Software/application, though there is potentially no restriction to offer multiple types at the same time, which can often be observed in PaaS (Platform as a Service) provider which offer specific applications too, such as Google App Engine in combination with Google Docs. Due to this combinatorial capability, these types are also referred as "components". The following list identifies the main type of clouds.

3.1. Cloud Infrastructure as a Service (IaaS)

It is also referred as Resource Code, provide (managed and scalable) resources as services to the user- in other words, they basically provide enhanced virtualization capabilities. Accordingly, different resources may be provided via a service interface.

3.1.1. Data and Storage Clouds

It deals with reliable access to data of potentially dynamic size, weighing resource usage with access requirements and/or quality definition. Examples: Amazon s3, SQL Azure.

3.1.2. Compute Clouds

It provide access to computational resource i.e. CPUs. So far, such low level resources cannot be exploited on their own, so they are typically exposed as a part of "virtualized environment". Examples: Amazon EC2, Elastic hosts.

3.2. (Cloud) Platform as a Service (PaaS)

It provides computational resources via a platform upon which applications and services can be developed and hosted. Example: Google Docs, SAP business by design.

3.3. (Clouds) Software as a Service (SaaS)

It is also sometimes referred to as Service or application clouds. These clouds are offering implementation of specific

business functions and business processes that are provided with specific cloud capabilities, i.e. they provide applications/services using a cloud infrastructure or platform, rather than providing cloud features them.

4. Fear of the Cloud

The Cloud Security Alliance's initial report contains a different sort of taxonomy based on 15 different security domains and processes that need to be followed in an overall cloud deployment. The security concerns can be categorized as: Traditional Security, Availability and Third-party Data Control.

4.1. Traditional Security

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Concerns in this category include:

VM-level attacks: Potential vulnerabilities in the hypervisor or VM technology used by the cloud vendors are a potential problem in multi-tenant architectures. Vendors such as third brigade mitigate potential VM-level vulnerabilities through monitoring and firewalls.

Phishing Cloud Provider: Phishers and other social engineers have a new attack vector as the Salesforce phishing incident shows.

Cloud provider vulnerability: These could be platform-level, such as SQL injection or cross site scripting vulnerabilities in salesforce.com

Expanded network attack surface: The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases.

Authentication and authorization: The enterprise authentication and authorization framework does not naturally extend into the cloud.

Forensics in the cloud: Traditional forensics methodologies permits investigators to seize equipment and perform detailed analysis on the media and the data recovered. The likelihood, of data being removed, overwritten, deleted or destroyed perpetrator in this case is low.

4.2. Availability: these concerns center on critical applications and data being available. Concerns in this category include:

Uptime: As with the traditional security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud user's own data centers. Besides, just services and applications being down, this includes the concern that a third-party cloud would not scale well enough to handle certain applications.

Single point of failure: Cloud services are thought of as providing more availability, but perhaps not- there are more single points of failure and attack.

Assurance of computational integrity: Can an enterprise be assured that a cloud is faithfully running a hosted application and giving valid results?

4.3. Third-party Data Control

The legal implications of data being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud. All this is prompting some companies to build private clouds to avoid these issues and yet retain some of the advantages of cloud computing.

Due Diligence: If served a subpoena or other legal action, can a cloud compel the cloud provider to respond in the required time-frame.? A related question is the provability of deleting relevant data to an enterprise's retention policy: how can a cloud user be guaranteed that data has been deleted by the cloud provider? Audit ability: Audit ability is another side effect of the lack of control in the cloud. Is there sufficient transparency in the operation of the cloud provider for auditing purposes?

Contractual obligations: One problem with using another company's infrastructure besides the uncertain alignment of interests is that there might be surprising legal implications.

Cloud provider espionage: This is the worry of theft of company proprietary information by the cloud provider. For example, Google, Gmail and Google Apps are example of services supported by a private cloud infrastructure. Corporate users of these services are concerned about confidentiality and availability of their data.

Data Lock-in: How does a cloud user avoid lock-in to a particular cloud computing vendor? The data might itself be locked in a proprietary format, and there are also issues with the training processes.

5. Critical Areas for Cloud Computing

The Cloud Security Alliance (CSA) has developed a 76-page security guide (Security Guidance for Critical Areas of focus in Cloud Computing) that identifies many areas for concern in cloud computing. This environment is a new model which cannot be well protected by traditional "perimeter" security approaches. From this document six specific areas of the cloud computing environment where equipment and software implementing TCG specifications can provide substantial security.

5.1. Securing data at rest

Cryptographic encryption is certainly the best practice and in many U.S states and countries worldwide, it's the law for securing data at rest at the cloud provider. Fortunately, hard drive manufacturers are now shipping self-encrypting drives that implement the TCG's trusted storage standards. Self-encrypting drives build encryption hardware in to the drive, providing automated encryption with minimal cost or performance impact.

5.2. Securing Data in transit

Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transmission.

5.3. Authentication

User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the internet.

5.4. Separation between Customers

One of the most obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines and a hypervisor to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation.

5.5. Cloud Legal and Regulatory Issues

To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, Trusted Storage and TPM access techniques can play a key role in limiting access to data.

5.6. Incident Response

As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response or at least automated notifications is the best solution.

6. Encryption Techniques

In cloud computing, it is frequent for the entities to communicate manually. To achieve the security in the communication, it is important to impose an encryption and signature schemes. Therefore, the following encryption techniques are proposed:

6.1. Identity Based Encryption

IBE is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. Compared with typical public key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators. An added advantage is that a message recipient doesn't need advance preparation or specialized software to read the communication.

How IBE works?

The success of IBE depends upon the third party IBE server that generates private keys. The only information this server stores permanently is a secret master key- a large random number that is exclusive to the security domain. The server uses this key to create a common set of public key parameters that are given to each user who installs the IBE software, and recipient's private keys are required.

When a sender creates an encrypted message, the IBE software on his system uses three parameters to generate the public key for the message: a starting value, the current week number and the recipient's identity. A user who receives an IBE encrypted e-mail message but has not used the process before can request- upon authentication- a private key that allows him to decrypt all e-mails encrypted using his e-mail address as the public key.

6.2. Linear Search Algorithm

In the Linear Search algorithm, a symmetric encryption algorithm is used to encrypt the plain text. For the cipher text of each keyword under symmetric encryption scheme, a pseudo-random sequence is generated with a length less that of the cipher text. Meanwhile, a check sequence is generated with a length less than that of the cipher text. Meanwhile, a check sequence is generated based on the pseudo random sequence and the cipher text. The sum of the lengths of the pseudo random sequence and the check sequence equals the length of the cipher text. Finally, the pseudo random sequence and the check sequence equals the length of the cipher text again by modulo 2 addition. When searching, a user submits the cipher text sequence under symmetric encryption schemes. On the server side, modulo 2 additions with each sequence is performed to each sequence. If the result satisfy the checking, the sequence is the encryption of the cipher text; otherwise, the sequence is not encryption of the cipher text.

6.3. Identity Based Signature

An identity based signature scheme is deterministic if the signature on a message by the same user is always the same. The framework of identity based signature scheme consists of algorithms described below:

Setup: The private key generator (PKG) provides the security parameter as the input to this algorithm, generates the systems parameters and the master private key.

Extract: The user provides his identity ID to the PKG. the PKG runs this algorithm with identity ID, parameters and master private key as the input and obtain the private key D. the private key D is sent to user through a secure channel.

Sign: For generating a signature on a message m, the user provides his identity ID, his private key D, parameters and the message m as input. This algorithm generates a valid signature on message m by the user.

Verify: This algorithm on input a signature on message m by the user with Identity ID, parameters, checks whether signature is valid on message m by ID.

6.4. Homomorphic Encryption

Homomorphic encryption alludes to encryption where plain texts and cipher texts both are treated with an equivalent algebraic function. Now the plain text and cipher text might also be not related but the emphasis is on the algebraic operation that works on both of them. Structured Encryption: A structured encryption scheme encrypts structured data in such a way that it can be queried through the use of a query-specific token that can only be generated with knowledge of the secret key. In addition, the query process reveals no useful information about either the query or the data. An important consideration in this context is the efficiency of the query operation on the server side.

6.5. Public Key Encryption with Keyword Search

A public key encryption with keyword search (PEKS) scheme consists of four polynomial time algorithms:

KeyGen: Take a input a security parameter and generate a public/private key pair (pk,sk).

Trapdoor: Take as input the receiver's private key sk and a word W, produce a trapdoor Tw.

PEKS: Take as input the receiver's public key pk and word W, produce a searchable encryption of W.

Test: Take as input the receiver's public key pk, a searchable encryption C=PEKS (pk,W').

6.6. Attribute Based Encryption

In ABE, the attributes and policies associated with the message and the user decides which user can decrypt a cipher text. A central authority will create secret keys for the users based on attributes/policies for each user.

Cipher text policy in ABE:

Users in the system have attributes; receives a key ("or key bundle") from an authority for its set of attributes. Cipher text contains a policy (a Boolean predicate over the attribute space). If a user's attribute set satisfies the policy, can use its key bundle to decrypt the cipher text. Multiple users cannot pool their attributes together.

7. Future Scope

There is a strong industry consensus that security, along with regulatory compliance is the barrier to the adoption of cloud computing. At the same time companies are attracted to cloud computing for its advantages: flexibility, elasticity and the pay-as-you-go economic model. Customers in the cloud can bring up servers and storage in minutes, and they expect a security solution which does not compromise the cloud values of flexibility and elasticity. The needed breakthrough should mean customer's data is always encrypted, and the master encryption keys are themselves encrypted, even when in use. Key splitting and homomorphic technologies are the secret sauce that can solve this challenge and this creates trust.

References

[1] H. Erdogmous, 2009. "Cloud Computing: Does nirvana hide behind the Nebula?" IEEE Software, vol 26.
[2] D. Boneh, 2008. "Generalization Identity based and broadcast encryption schemes". Vol 5350.
[3] Richard Chow, Phillepe Goel. "Controlling data in the cloud"
[4] http://ijcttjournal.org/volume-1/issue-2/ijcctjournal-v1i2p27.pdf
[5] http://eprint.iacr.org/2011/010.pdf
[6] http://crypto.stanford.edu/ibe/
[7] http://iac.dtic.mil/iatac/download/Vol13_No2.pdf
[8] http://www.computerworld.com/s/article/328729/Identity_Based_Encryption
[9] http://www.johnseelybrown.com/cloudcomputingpapers.pdf
[10] http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf
[11] http://www.davidchappell.com/CloudPlatforms--Chappell.pdf
[12] http://cloudcomputing.sys-con.com/node/1748825
[13] http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm Inc.