International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Review on Various Approaches of Data Security in Cloud Computing

Gurbachan Singh[1], Amandeep Kaur[2]

[1]Student, Desh Bhagat University, Mandi Gobindgarh

[2]Assistant Professor, Desh Bhagat University, Mandi Gobindgarh

Abstract: ***Cloud computing is a trending technology in the field of Information Technology as it allows sharing of resources over a network. The reason Cloud computing gained traction so rapidly was because of its performance, availability and low cost among other features. The proposed data security model provides user authentication and data protection. This makes certain secure communication system and hiding information from others. This model also includes onetime password (OTP) system for user authentication process. This structure can be easily applied with all cloud computing layers.***

Keywords: Cloud Computing, Availability, Cloud Security, Encryption

1. Introduction

1.1 Cloud Computing

Cloud computing is an innovative service mode. It enables users to get almost unlimited computing power and a variety of information services from internet. They are distributed computing, parallel computing and grid computational evolution. In cloud computing, all users' data are stored in the cloud resources nodes. The results distribute to the user through the network when the user needed. Although cloud computing has become a mature service model, and have large commercial, cloud computing is still facing many problems. In 2009, the well-known research institutions IDC release an IT report that cloud computing service is facing three major challenges: safety, stability and performance issue. Including the security problem concerns the most. A real cloud computing security incidents have profound reveals the self-healing urgency of cloud security issues, such as the 2009 Microsoft SIDEKICK service was interrupted for a week, a large number of users can not access to their email and other personal data. More seriously, due to the technical personnel not to make backups of their data, resulting in Microsoft cannot recover data. Although the cloud storage service can realize multi copy of fault tolerance and backup automatically, it also cannot do guaranteed 100% security. The use of cloud computing has increased rapidly in many organizations, for it offers potential benefits to users in terms of instant availability, scalability and resource sharing, while potentially posing security issues, problems of third-party data security and securely outsourcing computation become increasingly prominent. When moving services to the cloud, it can be both intimidating and terrifying for an enterprise to surrender control of its sensitive data and rely solely on a cloud computing service provider to keep it safe.

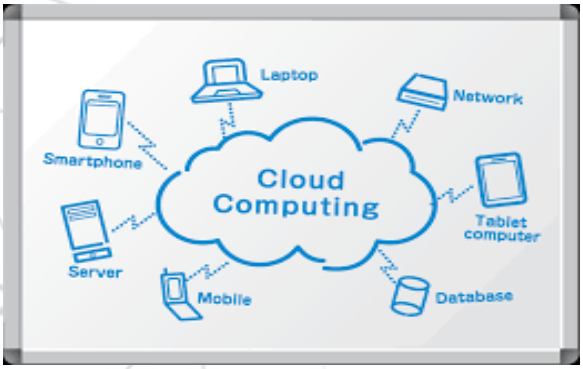

Figure 1.1: Cloud Computing

1.2 Service models of Cloud Computing

There are various models have been available for processing of cloud computing. In the processing of cloud computing basically whole process has been divided into three different models that are described below.

1.2.1 Software-as-a-Service

This was the earliest cloud service and the first to enjoy widespread adoption. In a nutshell, SAAS is the online delivery of software functionality and capability without the need for locally running software. Rather, SAAS runs on a Web browser.

1.2.2 Platform-as-a-Service

Broadly speaking a Platform-as-a-Service (PAAS) is a cloud-based application development environment. Using a PAAS, companies can produce new applications more quickly and with a greater degree of flexibility than with older development platforms tied directly to hardware resources. Running application development on a PAAS has number of key benefits. Programmers and development managers especially appreciate that the cloud provider handles all the care and maintenance of the underlying operating system(s), servers, storage, and application containers. PAAS environments can be extremely useful when development teams are widespread geographically or when partner companies or divisions share development efforts.

1.2.3 Infrastructure as a Service (IAAS)
Infrastructure Providers manage a large set of computing resources, such as storing and processing capacity. Through Virtualization, they are able to split, assign and dynamically re-size these resources to build ad-hoc systems as demanded by customers. They deploy the software stacks that run their services.

1.3 Deployment of Cloud Services

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud. There are four different deployment models of cloud computing:

1.3.1 Private cloud
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).

1.3.2 Community cloud
The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

1.3.3 Public cloud
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

1.3.4 Hybrid cloud
The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

1.4 Types of Cloud Computing

Cloud computing offers a variety of ways for businesses to increase their IT capacity or functionality without having to add infrastructure, personnel, and software. Seven different types of cloud computing are:

1.4.1 Web-based cloud services. These services let you exploit certain web service functionality rather than using fully developed applications. Like it might include an API for Google Maps, or for a service such as one involving payroll or credit card processing.

1.4.2 SaaS (Software as a Service). This is the idea of providing a given application to multiple tenants. SaaS solutions are common in sales, HR, and ERP.

1.4.3 Platform as a Service. This is saas variant. You run your own applications but you do it on the cloud provider's infrastructure.

1.4.4 Utility cloud services. These are virtual storage and server options that organizations can access on demand even allowing the creation of a virtual data center.

1.4.5 Managed services. In this scenario, a cloud provider utilizes an application rather than end-users. So, for example, this might include anti-spam services, or even application monitoring services.

1.4.6 Service commerce. These types of cloud solutions are a mix of SaaS and managed services. They provide a hub of services through which the end-user interacts. Common implementations include expense tracking, travel ordering, or even virtual assistant services.

1.5 Advantages of Cloud Computing

- **Lower-cost computers for users:** This point is one of the financial advantages of cloud computing. There is no need to purchase powerful and expensive equipment to use cloud computing since all the processing is not at your local computer but in the cloud.
- **Better performance:** Due to the fact that no programs or files are loaded on the local PC, users will not experience delays when switching on/off their computers and also the internal network will be much faster since no internal traffic will occur.
- **Less IT infrastructure costs:** The IT department of large organizations could experience decreasing on the expenses in regards with infrastructure with the adoption of the cloud computing technology.
- **Less maintenance costs:** Maintenance costs also will be reduced using cloud computing since both hardware and software maintenance for organizations of all sizes will be much less
- **Lower software costs:** Using cloud computing there is no need to purchase software packages for each computer in the organization, only those employees actually using an application need access to that application in the cloud.
- **Automatic software updates:** All the software's need update and the great thing with cloud computing is that you do not have to worry for any updates and also your organization will not have any additional expenses when a new upgrade or update is necessary.
- **Increased computing power:** When using cloud computing, you can use the cloud computing power since you are no longer limited to what a single desktop computer can do.

2. Review of Literature

A lot of work has been done on Fully Homomorphic Encryption technique. After reviewing all the papers, we come to know that .The main problem occurring is regarding security of data.

Darko Hrestak et al. [1] Since the first notions of fully homomorphism encryption more than 30 years ago, there has been numerous attempts to develop such a system. Finally, in 2009 Craig Gentry succeeded. Homomorphism encryption brings great advantages but it seems that, at least for now, it also brings many practical difficulties. Furthermore, in the last couple of years, several other fully homomorphism systems arose where each has its one advantages and drawbacks. However, with the developments in cloud computing, we need it more than ever to become practical for real-world usages.

Hongchao Zhou et al. [2] Homomorphic encryption, aimed at enabling computation in the encrypted domain, is becoming important to a wide and growing range of applications, from cloud computing to distribute sensing. In recent years, a number of approaches to fully (or nearly fully) homomorphic encryption have been proposed, but to date the space and time complexity of the associated schemes has precluded their use in practice. In this work, we demonstrate that more practical homomorphic encryption schemes are possible when we require that not all encrypted computations be supported, but rather only those of interest to the target application.

Feng Zhao et al. [3] with the rapid development of Cloud computing, more and more users deposit their data and application on the cloud. But the development of Cloud computing is hindered by many Cloud security problem. Cloud computing has many characteristics, e.g. multi-user, virtualization, scalability and so on. Because of these new characteristics, traditional security technologies can't make Cloud computing fully safe. Therefore, Cloud computing security becomes the current research focus and is also this paper's research direction.

Jian Li et al. [4] with continuous expansion of cloud computing, problems of third-party data security becomes increasingly prominent. However, effective retrieval of encrypted data and other operations are difficult to achieve by traditional cryptogram systems. Thus, a practical simple fully homomorphism encryption scheme, using only elementary modular arithmetic, derived from Gentry cryptosystem is put forward to ensure the privacy-preserving in cloud storage, in which encrypted data can be operated directly without affecting the confidentiality of the encryption systems, so that it can excellently realize the need of chipper-text retrieval and other processing in un-trusted servers.

Y Govinda Ramaiah et al. [5] Fully Homomorphism Encryption has become a hot research topic in light of the privacy concerns related to the emerging cloud computing paradigm. Existing fully homo-morphic schemes are not truly practical due to their high computational complexities and huge message expansions. Targeting the construction of a homomorphic encryption scheme that is implementable for at least certain class of applications, this paper proposes a Somewhat Homomorphic public key encryption scheme, which can be viewed as a variant of the scheme.

Hao-Miao Yang et al. [6] At Euro crypt 2010 van Dijk et al. presented a very simple somewhat homomorphic encryption scheme over the integers. However, this simplicity came at the cost of a public key size in O_ __10 _. Although at Crypto 2011 Coron et al. reduced the public key size to O_ __ 7 _, it was still too large for practical applications. In this paper we further reduce the public key size to O_ __ 3 _ by encrypting with a new form.

Ahmed Dheyaa Basha et al. [6] currently, mobile application and computing is gaining a high momentum and playing a significant role in enhancing the internet computing infrastructure. In addition, the mobile devices and their applications have high technique in the service ever had, and developed rapidly. Mobile cloud computing is expected to generate significantly more innovative with multi applications.

3. Approaches Used

3.1 The RSA Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.
Using an encryption key (e,n), the algorithm is as follows:

1) Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2) Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.
3) To decrypt ciphertext message C, raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
2. Set n equal to $p * q$.
3. Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
4. Find e such that $e * d = 1$ (**mod** ((p-1) * (q-1)))

3.2 (Fully Homomorphism Encryption) FHE

Homomorphism encryption schemes permit anyone to evaluate functions on encrypted data, but the evaluators never see any information about the result. All known FHE schemes are based on the hardness of lattice problems. Some of the applications of FHE do not require its full power – for PIR, it is sufficient to have a somewhat homomorphic encryption scheme capable of evaluating simple database indexing functions. A homomorphic encryption scheme
FHE :=(KeyGen; Enc; Dec; Eval) is fully homomorphic if it satisfies the following properties:
1. Homomorphism: Let CR = $\{CR_\lambda\}\lambda \in N$ be the set of all polynomial sized arithmetic circuits. On input sk ←KeyGen(1^λ),∀ckt ∈ CR_λ,∀(u_1,…, u_n)∈Fq^n where n = n(λ), ∀(c_1,…,c_n)
Where c_i← Enc(sk;u_i, it holds that:
Pr[Dec(sk;Eval(ckt; c_1,…,c_n)) ≠ ckt(u_1,…, u_n)] = negl(λ).

2. Compactness: There exists a polynomial $\mu = \mu(\lambda)$ such that the output length of Eval is at most μ bits long regardless of the input circuit ckt and the number of its inputs.

3.3 One Time Password) OTP

For login-in to the cloud, user will enter his user name and one time password (OTP) which has been generated on its mobile phone, on to login page. This user name and one time password will then send to server for authentication. At server side, it will also generate one time password and will match with the received one time password. If received OTP and server generated OTP are same, then only user will allowed to login to the cloud otherwise its access will be denied.

i) OTP offers strong two-factor authentication.
ii) The OTP is unique to this session and cannot be used again
iii) OTP offers strong security because they cannot be guessed or hacked
iv) Provides protection from unauthorized access Easier to use for the employee than complex frequently changing passwords
v) Easy to deploy for the administrator Good first step to strong authentication in an organization
vi) Low cost way to deploy strong authentication.

3.4 Blowfish: Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention.Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries

4. Conclusion

As the data on the cloud is accessible publicly some kind of security mechanism needs to be there so that only trusted people can be given access to the cloud. Data is encrypted using some type of encryption. This can be achieved by using OTP (One Time Password). OTP is generated at each login and it is sent to the party's registered mobile or email address. Using the OTP, one can successfully login. Here Fully Homomorphic Encryption (FHE) comes into picture. In this approach data is encrypted using Fully Homomorphic Encryption. The homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions, and private information retrieval schemes and enable widespread use of cloud computing by ensuring the confidentiality of processed data.

References

[1] Darko Hrestak "Homomorphism Encryption in the Cloud", ISSN 978-953-233-081-6, pp.1400 – 1404, IEEE, 2013.
[2] Hongchao Zhou "Efficient Homomorphic Encryption on Integer Vectors and Its Applications", ISSN 14255976, pp. 1 – 9, IEEE, 2014.
[3] Feng Zhao "A cloud computing security solution based on fully homomorphism encryption", ISSN 978-89-968650-2-5, pp. 485 – 488, IEEE, 2014.
[4] Jian Li "A Simple fully homomorphic encryption scheme available in cloud computing", ISSN 64753, Vol 01, IEEE, 2014.
[5] Y Govinda Ramaiah "Efficient Public key Homomorphic Encryption over Integer Plaintexts", ISSN 978-1-4673-2588-2, IEEE, 2012.
[6] Hao-Miao Yang "A cloud computing security solution based on fully homomorphic encryption", ISSN 978-0-7695-4639-1, IEEE, 2014.
[7] Ahmed Dheyaa Basha, Irfan Naufal Umar, and Merza Abbas, Member, IACSIT "Mobile Applications as Cloud Computing: Implementation and Challenge", ISSN 7865-7564, IEEE, 2013.
[8] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing
[9] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing
[10] Ru Wei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Research on Privacy-Preserving Cloud Storage Framework Supporting Cipher text Retrieval" 2011 Ninth International Conference on Grid and Cloud Computing.