Indian Journal of Science and Technology, *Vol 10(6), DOI: 10.17485/ijst/2017/v10i6/98546, February 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhanced Methods to Provide Privacy from Massive Surveillance

N. Gowtham Kumar[1]*, Niranjan Polala[2] and D. Aruna Kumari[3]

[1]Computer Science and Engineering, KL University, Vijayawada - 522502, Andhra Pradesh, India; gowtham520@yahoo.com
[2]Department of Computer Science and Engineering, KITS, Warangal - 506009, Telangana, India; npolala@yahoo.co.in
[3]Department of Electronics & Computer Engineering, KL University, Vijayawada - 522502, Andhra Pradesh, India. aruna_d@kluniversity.in

Abstract

Background/Objectives: The recent revolution in information technology has had a major impact on Global Communication. The use of Cloud computing in many organizations has significantly increasing due to the benefits in terms of accessibility and inexpensive in general. Due to these anticipated advantages of Cloud Computing many companies and users do not analyze the security issues carefully. **Methods/Statistical Analysis**: The unprecedented massive surveillance carried out by unauthorized parties around the world threaten cloud users. Offering strong data protection and build confidence to rich applications in the cloud is a challenging task. To mitigate technical impediments in cloud this paper suggested some available security prepositions. **Findings:** This paper mainly focuses on various propositions such as protecting virtual infrastructures, use of proxies and SSH tunneling, Disk encryption to provide protection for the data at rest, Homomorphic encryption to provide confidentially to the data in transit and finally data integrity to check whether data modified at cloud servers, to take care of privacy and freedom of data of Cloud users while adapting to cloud. **Applications/Improvements:** These security prepositions may ensure in increasing the trust to incorporate the user services on the cloud beyond the shadow of the doubt.

Keywords: Data Integrity, Encrypted, Homomorphic Encryption, Multi-Tenancy, Massive Surveillance, Side Channels Attacks, Tunneling

1. Introduction

The term "Cloud computing" becomes popular as probable cost savings to the cloud service provider (CSP) from outsourcing data. As the cloud is gaining more popularity, many organizations want to move towards the cloud, but security is the key concern. Cloud users would have lots of questions about the secrecy of their data. Including these, there are many government compliances, reliability, and complexity issues arise.

In a **Public Cloud,** services are operated and owned by Cloud Service Provider (CSP) through the use of the Internet. For example, some services focus on enterprise such as Sales force, Microsoft Azure, AWS and in addition few services such as social networking, e-mail, photo storage services which are accessible to the general public. In a **Private Cloud**,

*Author for correspondence

cloud infrastructure for a particular organization operated and maintained by an individual or a third party, examples such as Windows Azure and Open Stock. A group of organizations shared their services and made available only to those organizations through **Community Cloud**, providing infrastructure may be claimed and controlled by them or CSPs. Combination public and community clouds are possible through **Hybrid Cloud** such as Microsoft "Cloud OS" [1].

Based upon using above types, numerous security concerns need to be considered.

Multi-tenancy is a key issue, as same resources are shared by users and co-location of VMs on a single server may increase the threat/attack surface. It is very difficult to CSPs to enforce uniform security controls, measures and mutual client isolation.

Security threats upgrade and spread rapidly in cloud named as Velocity of Attack (VOA) factor. Generally the cloud infrastructure is moderately outsized; unmistakably the surface of attack is moreover high. This may provoke to potential disaster and ends up being greatly fundamental to reduce the spread of the attack. CSP necessities to take up more competent security execution systems to against such attack.

To provide the Information assurance and data ownership, Client's private data (such as client's identity, service details, etc.) are hoarded, maintained and accessed by CSP. However, CSP is not the legitimate owner of that data may lead to potential unauthorized data access and also misuse of sensitive information. Hence, data have to be protected by providing the services like confidentiality and access control mechanisms.

As per Garter overview, worldwide spending on public cloud services is relied upon to grow 18.6% in 2012 to $110.3B, accomplishing a compound annual growth rate (CAGR) of 17.7% from 2011-2016. By the end of 2016 from 2010 the aggregate IaaS market may reach from $76.9B to $210B[2]. The SaaS market between 2015-2018 is anticipated to develop from $49B to $67B with a 8.14% growth rate. At the end of 2016, IaaS is relied upon to achieve $16.5B. By the year 2019, mobile data traffic makes use of cloud applications almost 90% around the world with 60% of annual growth rate[3]. Table 1 below shows the market share of IaaS in 2015.

Table 1. 2015 IaaS Market Share

S.No	Orgnization	Market Share
1	Sales Force	24%
2	Amazon	17%
3	Microsoft	10%
4	IBM	3%
5	Service Now	3%
6	Google, Oracle, Netsuite	Each one 2%
7	Others	37%

Moving data into the cloud frees the issues of administration of assets of clients of their own, for instance, Amazon S3 (Simple Storage Service) and Amazon EC2 (Elastic Compute Cloud) are both well-known cloud vendors[4]. Cloud-hosted web services are vulnerable,as physical infrastructure normally shared by different clients. To make the single data protection is unbelievable in the cloud as it includes applications like personal financial management, e-mail, social networks, and tools like word processors and spreadsheets.

In this paper, section 2 presented security importance, risk and threats in a cloud computing environment. Section 3 presented the relation among trust and cost to utilize clouds. Section 4 introduced five security prepositions to mitigate cloud security breaches. Finally, the conclusions and further work were shown in the last portion.

2. Providers and Data Security

Cloud computing providing utility oriented IT services that empower facilitating of applications from scientific and business around the globe based on a "pay-as you-go" model to consumers.

As per IDC survey the top challenge for 74% of CEOs is cloud security[5]. With reference to Microsoft soft survey, due to benefits getting from cloud 86% of industry expert and 58% of the public were delighted as lower cost, less overhead management and accessibility, yet more than 90 percent of them are made a big deal about security, and accessibility of their information as it rests in the cloud.[4]. To adopt the cloud, the key issue to the companies is "lack of trust". The consumers will be in trouble, if

the companies have not taken proper security measures to protect their own environments[6]. However, predicting the quality of security that the CSPs are providing is difficult because they are not completely exposing their Infrastructure.

According to Alert Logic's Annual Cloud Security Report 2014, as shown in Figure 1 below various attacks experienced in the Cloud Hosting Provider environments, each impacting over 40% of the cloud hosting base[7].

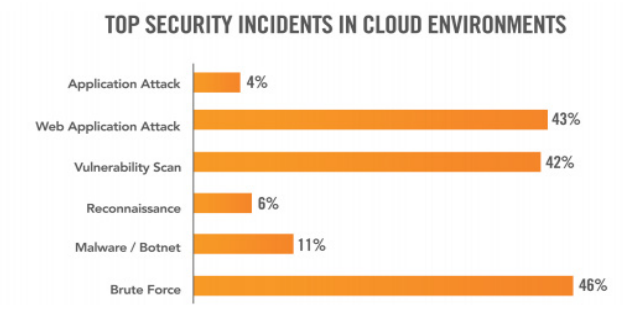

Figure 1. Logic's Annual Cloud Security Report 2014.

Privacy is a fundamental right of every individual. One of the biggest issues in Cloud is data integrity and confidentiality; the data hoarded at the cloud provider, could suffer from damage or eavesdropped by the intruders. 175 million clients of LinkedIn, revealed that their secret key database was traded off,around 6.5 million hashed passwords were stolen and posted onto a Russian web forum and more than 200,000 of these passwords have been broken. In addition Dropbox has affirmed that its clients experienced a spam assault. Usernames and passwords stolen from different sites were utilized to sign and recover Dropbox clients' records with e-mail addresses to sent spam messages about online casinos and gambling sites to various clients[8].

A group of security specialists found that the Drown protocol is an example of 'cross-protcol attack' that make use of one protocol such as SSLv2 to attack another protocol,in this case TLS, security of connections[9].Prevously Bleichen Bacher proposed an amazing attack on a SSLv2 encryption scheme that allows an attacker to decrypt an RSA cipher text efficiently without having private key of the legitimate user.

In 2009, a complaint received that, due to malfunction of softwaretheuserdatagotunauthorizedaccessatcloudprovider which prompted an investigation on Google's Cloud Computing Services by the Electronic Privacy Information Centre (EPIC) plea with Federal Trade Commission to identify the effectiveness of privacy and security measures. Also, there is another risk on data integrity due to the provider's defect, whichfound a flaw in Amazon S3 where users were confused due to unexpected data corruption[10].

Through Elastic search, cyber-criminals have been launching DDoS attacks from cloud-based bots, according to researchers[11].Taking information put away on Cloud could happen on Social Networking Sites, have pulled in individuals who collaborate with companions in their regular day to day existences.These systems give a stage to clients to impart data to others, e.g. individual profile (phone, birth-date

gender, email,etc) and computerized media (photographs, music,etc). However, if the attackers find a way to gain over the cloud, the private data can possibly be hacked by them.

Insider attacks can be executed by malicious employees at the service provider's location can break the trust of clients. An insider can without much of a stretch acquire passwords, crypto-keys and documents. These attacks may incorporate different sorts of extortion, harm or robbery of data and abuse of IT assets. Because of the absence of straight forwardness in provider's procedures and methods the impact of threat of malicious attacks has grown. Also, clients have less perceivability about the enrolling practices of their provider that could open the gateway to intruders to take secret data or to get entrance over the Cloud.[12]

In a cloud environment, the cloud users (tenants) are isolated logically, but physically integrated. The extent of logical isolation must be intact, where the extent of physical integration will deviate. Even though additional physical integration is provided, preserving logical isolation becomes difficult. A query rewriter is used by Salesforce.com at the database level. Hypervisors are used at the hardware level by Amazon[13]. The Data holders facing competition for shared rudimentary resources among numerous applications.

CSA conducted a survey to identify the top threats within cloud computing and make out critical threats ranked in order of their severity: Data Breaches and Loss, Account Hijacking, Insecure APIs, Malicious Insiders, Denial of Service,etc.

3. Trust and Risk

Cloud computing risk assessment report conducted by The European Network and Information Security Agency (ENISA)'s state that as a top risk of cloud computing, especially for Infrastructure as a service(IaaS) is "loss of governance"[4].

Trust and risk are the opposite sides of the same coin. Trust is important in the notion of accountability. Risk is a measure of vulnerability. Due to loss of control, if the amount of cost benefits getting from moving services to cloud might be very less than the amount of cost that was actually invested. In such a situation, it becomes worst to the cloud users.

At present the people have not confidence in online services compared to offline, as these services may not establish centralized authorities in a proper way. Some researchers would argue that security is not even a component to distinguish the degree of the trust and other contended that the level of security does not reflect the trust. Individuals will use an eCommerce if their credit-card details and personal information are cryptographically ensured that prompts to trust developing among them[14]. There are numerous service providers in cloud coexist and collaborate to provide their services, so it must address heterogeneity among their policies as they may have distinctive security methodologies and protection systems.

4. Some Propositions for Security in Cloud Computing

The core issue is that cloud provider is also has some control of the user's data. In this section, we discuss some security approaches that may be utilized at the time of cloud computing deployments while limiting the provider's control, on data.

4.1 Protecting Virtual Infrastructures

Even though business organizations are promising efficiency and agility within the cloud, still it requires visibility and control in their data centers. As more business-critical applications move to the cloud, the need for high availability becomes increasingly important.

A group of researchers at various universities and RSA Laboratories has explored recently, side channel attacks on virtual machines and virtual networks created in the cloud on behalf of cloud users. With these attacks, one virtual machine can use against another one, with the target VM's encryption key ultimately being compromised within a cloud environment. So confidential data that had been encrypted with the target VM's key could be compromised, resulting in heavy loss to cloud users. To perform the side channel attack requires placement (i.e. the malicious virtual machines are placed on the same physical machine by the intruder) and extraction (once the placement of the malicious VMs is completed fruitfully, then confidential documents and files are extracted which are on the target VM by the malicious VM).

In general, it is very difficult to launch the side-channel attacks without detailed knowledge of the environment and some of the detail of and control over the hypervisor infrastructure and VMs in use on these platforms. However, there are some initial steps taking to mitigate the risk of future side-channel attacks should consider that concerned organizations. As a first step, locks down the Operating System (OS) images and application instances as much as possible to prevent compromise of any vectors in the environment. Second, dedicate time, to modify, collecting local processed monitoring data and logs for cloud systems. Other than these steps, code the applications including OS components as such a way shared resources can access similar to memory cache in a consistent, predictable way. This can prevent attackers from collecting harmful information potentially, for instance, timing statistics and other behavioral attributes[15].

4.2 Proxy and Encrypted Tunneling

It is necessary to understand how some technologies to protect the data online. This section describes various issues such Tor, Proxy, Virtual Private Networks (VPNs). The Tor Cloud project developed a user-friendly way of locating bridges on the Amazon EC2 cloud computing platform to provide user's access without being examined the Internet. By sending data through the Tor's servers, it becomes unfeasible for online entities see where the data originated from. In theory, that all sounds good and well. However, as a result of various bugs it has steadily declined since early 2014.

A proxy server is an intermediary device used to access web content by redirecting the traffic (for both inbound and outbound data). Each CSP within its cloud infrastructure can host proxies to handle service requests from clients[16]. A proxy may efficiently cache the data and serve data to other nearby proxies. It also caches

intermediate results from a cloud interaction that may be reused again.

SSH tunnel is created an encrypted channel by making use of an SSH connection protocol. Through this encrypted channel allows an unencrypted data (plain data) is tunneled over a network. In a simple language, it maintains regular surveillance around the contents of net and also surf blocked sites. Enterprise IT owners worldwide use VPNs to meet the connectivity needs of their businesses with security, availability and performance. The difference between proxy and VPN is everything in a VPN is encrypted that provide an additional layer of security.

4.3 Disk and Database Encryption

Disk encryption is in a general sense concentrating on securing information by changing over data into ciphertext, which can't be decoded by unauthenticated parties effortlessly. In this process,encrypt all of the data every bit) that lying on a disk volume by the disk encryption programming or hardware.Tim Rains (Chief Security Advisor Worldwide Cyber security and Data Protection) express that there are many controls accessible, regardless of whether the information is put away on online or offline**.**There are different classes of threats are possible while the information is to consider in an inert mode,- such as - i) Processed and stored massive cloud storage data compromised and gain access over the data by the attackers ii) information related to the customer supposed to theft by a malicious or rogue administrator that contains in a physical disk drive. iii) Without the knowledge of the customers, the government may give a warrant to get to/recover the client's information.

Raluca Ada Popa et al proposed CryptDB, a system to offer secrecy to applications by applying SQL queries on the DBMS server against encrypted data. CryptDB addresses two threats. i) A curious database administrator (DBA) will try to take a closer look on the individual's data, such as financial statements, health records, and personal information as gaining the control over the DBMS server. In this case, it tries to inhibit the DBA from learning private data. ii) An intruder able to gain the complete control of application and DBMS servers.In such case, during an attack CryptDB can't give any guarantee to clients who are as of now log into the application, yet at the same time it gives secrecy of logs-out clients' information[17]**.** Luca Ferretti et. Al proposed MuteDB, an architecture that guarantees data isolation and confidentiality on any relational cloud database service rented by a tenant organization [18].

4.4 Homomorphic Encryption

Homomorphic encryption methods make use of complex mathematical operations to perform encryption or decryption methods applied on data without any loss of security. Most of the researchers concerning Homomorphic encryption, in the future, is expected to play a crucial role in cloud data security, by taking the vast advantage of the cloud provider's analytic services, in turn, most of the companies will attempt to hoard and the encrypted data that should be kept in public cloud.

When a single modification is required to the client's encrypted data, the client has to share the common key with the Cloud provider. Again, this sharing will lead to exploitation of data. To overcome this, Homomorphic Encryption systems, has given the secret key to the client and are able to perform various operations on encrypted data without sharing the private key with Cloud provider[4,19].

Below Figure 2 shows procedure of Homomorphic Encryption.

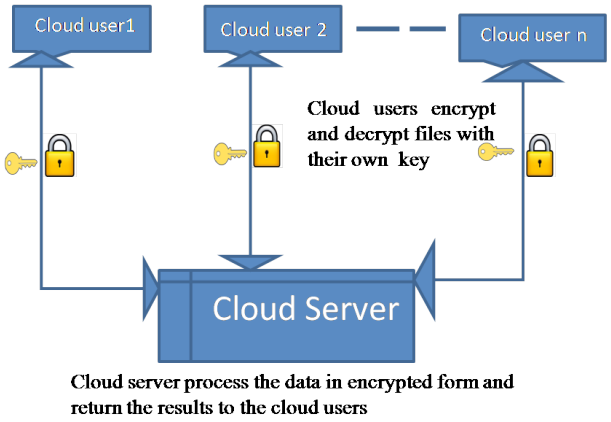

Figure 2. Homomorphic Encryption.

Homomorphic Encryption Two types: 1) Fully Homomorphic Encryption (FHE), which allows encryption for the client's data by providing an unrestricted, random number of computations (both addition and multiplication). 2) Some What Homomorphic Encryption(SHE) underpins a limited number of operations (i.e., any amount of addition, but only one

multiplication) and are speedier and more conservative than FHE cryptosystems[15].

With Homomorphic encryption, the web-client would send encoded data to a cloud server, which would deal with it without unscrambling and send back same encrypted data[20].

4.5 Proofs of Storage

In public cloud environment, clients, store their massive data and applications in Public Cloud Storage (PCS) Servers at diversified locations. These Cloud Servers are semi-trusted, as even well-known cloud platforms may experience malicious attacks and hardware/software failures. Using a proof of storage, a client can be able to verify whether the cloud provider has exploited and/or tampered with his data. To perform this task client may not require a local copy of data and also it is not required to get back the data from database. Actually, this work is very small for the client compared to the huge data and applications which are at provider's hand. It is most useful when a client can make use of some commercial public cloud storage services which provides scalable as well as dynamic storage services such as Microsoft's Azure and Amazon's S3.

Recently, many mechanisms [21-27] have been proposed on data integrity auditing .These methods allow a Third Party Auditor (TPA)(one who provides expert and provable integrity checking) on behalf of a data owner. The auditor could perform random integrity checking on a piece of small blocks without making use of the owner's entire data hoarded at provider's database. In some these mechanisms, data is divided into small chunks or blocks and the owner could make use of digital signatures to sign. All these public auditing solutions focus on personal data in the cloud.It is also necessary to reduce the trust on the auditor to improve data integrity auditing effectiveness and preserve the shared data on the cloud is unmodified.

5. Conclusion and Further Work

The need of providing security to the data becomes increasingly urgent, as huge private data move online. The suggestions made here provide confidentiality and data integrity in a traditional clouds environment, keeping in mind that clouds users who make use of CSP. However, many practical questions preclude such as interoperability, SLA and Legal issues still remain, particularly in a federated cloud environment where multiple CSPs are integrated to provide 'infinite' pool of resources. In future, it is necessary to concentrate on user centric cloud security where cloud users are roaming with handheld devices to get their services without interruption and interception.

6. References

1. Kirubakaramoorthi R., Arivazhagan D, Helen D. Analysis of Cloud Computing Technology. Indian Journal of Science and Technology. 2015; 8(21):1–3. https://doi.org/10.17485/ijst/2015/v8i21/79144
2. Public Cloud Services Market Sector. 2013 Feb 19. Available from: http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth.
3. Roundup Of Cloud Computing Forecasts And Market Estimates Q3 Update, 2015. 2015 Sep 24. Available from: http://www.forbes.com/sites/louiscolumbus/2015/09/27/roundup-of-cloud-computing-forecasts-and-market- estimates-q3-update-2015/#50d8e88b6c7a.
4. Dawn Song, Elaine Shi, Ian Fischer, Umesh Shankar. Cloud data protection for the Masses. IEEE Computer Society. 2012; 45(1):39–45. https://doi.org/10.1109/MC.2012.1
5. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom. Cloud computing security: From Single to Multi-Cloud. 45th Hawaii International Conference on System Sciences. IEEE 2012, pp. 5490-5499.
6. Sainy pearson. Toward accountability in the cloud. HP lab, IEEE Cloud Computing . 2013 May/June; 15(4): 64–9.
7. Shared Responsibility of Cloud Security. 2015 May 20. Available from: http://www.sureskills.com/about/blog/training_certification/the-shared-responsibility-of-cloud-security.
8. Te-Shun Chou. Security Threats On Cloud Computing Vulnerabilities.International Journal of Computer Science and Information Technology (IJCSIT) 2013; 5(3): 79–88. https://doi.org/10.5121/ijcsit.2013.5306
9. Nimrod Aviram. DROWN: Breaking TLS using SSLv2. Proceedings of the 25th USENIX Security Symposium. 2016 August;1–18.
10. Amazon S3 Silent Corruption. 2009 Jan 28. Available from: Sun. http://blogs.sun.com/gbrunett/entry/amazon_s3_silent_data_corruption
11. DDoS–ers-launch-attacks 2014 July 20. Available from:
12. Zulkefli Mohd Yusop, Jemal H. Abawajy. Analysis of Insiders Attack Mitigation Strategies. International Conference on Innovation, Management and

Technology Research,Malaysia. 22 – 23 September, 2013. PMCid:PMC3786081
13. Hassan Takabi ,James B.D. Joshi,Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE . 2010 Nov/Dec; 8(6):24–31.
14. Siani Pearson . Privacy, Security and Trust in Cloud Computing. 2012. Available from:
15. Research Directorate staff. Securing the cloud with homomorphic encryption. The Next Wave. 2014; 20(3):1–4.
16. Solmaz, Vaghri, Mohan KG. Using proxies to facilitate collaboration in Multi-Cloud Computing Environments. International Journal on Advanced Computer Thoery and Engineering. 2014; 3(2): 2319-2526,27–33.
17. Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, Hari Balakrishnan . CryptDB: Protecting Confidentiality with Encrypted Query Processing. MIT CSAI. 23rd ACM Symposium on Operating Systems Principles (SOSP), Cascais, 2011 Oct;1–16. https://doi.org/10.1145/2043556.2043566
18. Luca Ferretti, Fabio Pierazzi, Michele Colajanni, Micro Marchetti. Scalable Architecture for Multi-user Encrypted SQL Operations on Cloud Database Services. IEEE Transactions on Cloud Computing, 2014 Oct-Dec; 2(4): 448–58. https://doi.org/10.1109/TCC.2014.2378782
19. Maha Tebba, Karim Jkik, Said EL Hajii. Hybrid Homomorphic Encryption Method for protecting the privacy of banking Data in the Cloud. International Journal of Security and Its Applications. 2015; 9(6):61–70. https://doi.org/10.14257/ijsia.2015.9.6.07
20. Securing the cloud. 2013 Jan 10. Available from: http://news.mit.edu/2013/
21. Jothi Neela T., Saravanan N. Privacy Preserving Approaches in Cloud: a Survey. Indian Journal of Science and Technology. 2013; 6 (5):4531–5.
22. Erway C, Kupcu A, Papamanthou C, Tamassia R. Dynamic Provable Data Possession. Proceedings of the 16th ACM Conf. Computer and Comm. Security (CCS'09). 2009;213–22. https://doi.org/10.1145/1653662.1653688
23. Wang Q., Wang C., Li J., Ren K, Lou W. Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing. Proceedings of the 14th European Conference Research in Computer Security (ESORICS'09). 2009;355–70. https://doi.org/10.1007/978-3-642-04444-1_22
24. Wang B., Li B., Li H. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. Proceedings of IEEE Fifth International Conference Cloud Computing. 2014; 2(1): 43–56.
25. Rajathi A., Saravanan N. A Survey on Secure Storage in Cloud Computing. Indian Journal of Science and Technology. 2013; 6(4):4397–401.
26. Wang C., Wang Q., Ren K., Lou W. Ensuring Data Storage Security in Cloud Computing. Proceedings of the17th International Workshop Quality of Service (IWQoS'09). 2009; 5(2): 1–9. https://doi.org/10.1109/iwqos.2009.5201385
27. Wang C., Chow S.S., Wang Q., Ren K., Lou W. Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions Computers. 2013; 62(2):362–75 https://doi.org/10.1109/TC.2011.245.