Cloud Computing Security and Privacy Issues: Comparative Study

Y. M. Wazery[-1]A. H. Fawzy[-2]H. Meldeen[-3]
1- Department of information technology, Faculty of computer and information, Minia university
2,3 Department of information systems, Faculty of computer and information, Minia university

Abstract

Cloud computing is an important technology that transform centralized resources to shared resources ,it is a collection of IT resources including hardware and software serving multiple consumer which becomes essential process to organizations , business and operations , so cloud computing added many features such as the elimination of expenses associated with IT infrastructure management, space and energy. Cloud computing enables access to resources from any end device anywhere via the internet, it also provides high storage and computing services and facilitates innovation, this paper discuss security issues and different challenges that faced cloud computing such as privacy preserving issues and their solutions.

Key words: *cloud computing, cloud computing service models, security issues and privacy issues*

I. INTRODUCTION

Cloud computing is an important technology to discuss, the organizations are looking for the cloud computing as the essential process of their business and operations, cloud computing is the delivery of computing services, servers, storage, databases, networking, software, analytics and more cross the internet, it allows the customers and business to use applications without installation and access their personal file from any computer across the internet, cloud computing influential means of attaining high storage and computing services at a low cost, most cloud computing services fall into three broad categories : infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), These sometimes call cloud computing stack because they build in top of one another.

IaaS: enable the customer to focus on the core business rather than the underlying infrastructureby provision processing, networks, storage, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications, Example: Google APPs, Microsoft office.

PaaS: enable the customer to manage development and deployment environment byprovision compute, storage, libraries, a database, a programming framework, programming languages, operating system and other hardware and software tools to develop, test, deploy, applications, Example:Microsoft Azure PaaS, Google App Engine.

SaaS:enable the customer to drop the installation on end devices, which can access the applications from anywhere and use it through a web browser as a web service on a different end devices, Example: Dropbox, Office 365.

The five essential characteristics of cloud computing are:

1. On demand self-services: enable the customer to get computing capabilities such as server time and network storage without requiring human interact with service provider.
2. Resource pooling: enable to serve multiple customer, which can improve resource utilization and dynamically assigned and reassigned according to customer requirement.
3. Broad network access: enable customer to access cloud services on any device from anywhere via the internet.
4. Rabid elasticity: enable resources to appear as unlimited and can be provisioned in any quantity at any time, which provide the ability for customer to quickly request, receive, and release resources as needed.
5. Measured service: enable the resource usage to be monitored, reported, and controlled using the metering system involved in Cloud infrastructure, which can generate bills of cloud service used by customer.

Now we will discuss some of the advantages of cloud computing:

There is no doubt that businesses can collect huge services from cloud computing with the many advantages.

1. A. Cost savings

Enable the customer to hire from the cloud only resources, which eliminate the expenses associated with IT infrastructure management, space, energy. Businesses, no problem what their type or size, exist to reap money while keeping capital and operational spending to a minimum. With cloud computing, you can keep fundamental capital costs with zero in-house server storage and application requirements.

B. High availability

Provide the ability to ensure resource provisioned based on customer requirement,
And enable fault tolerance.

C. Flexible

Access Enable the customer to eliminate dependency on specific end point, in cloud infrastructure the application installed on provider premises and can be accessed from any end point over the network.

D. Manageability

Enable provider to enhanced and simplified management capabilities of resource, vendor managed infrastructure and SLA back agreement.

E. Business agility

Enable the capability to provision resource quickly and at any time with reduce the time required to deploy new services, which facilitate innovation by enable rabid development.

F. Application development and testing

Enable the organization to test application under different environment by create compute system in different hardware and software configuration.

G. Simplified Infrastructure Management

Enable organization to manage only resources that are required to access the cloud infrastructure, the cloud infrastructure is managed by the provider.

II. RELATED WORK

In [1] the author discuss the Cloud Security Issues that are classified as Data Issues, Privacy and legal issues and malicious application**,** Privacy Preserving and public auditing schema, in this paper, theoretical analysis of various kinds of security threats and various issues that affect the privacy preservation of the data users are done. Also the methods used to solve the security threats are discussed. Different ways to solve the issues that are preventing the privacy preservation are also analyzed. Various types of solutions to overcome these issues are discussed, and discusses Different cryptographic mechanisms that are used to resolve the security threats are specified such as Public Key based Homomorphic Linear Authentication (HLA) This scheme presents Privacy Preserving and Public Auditing for Data in Cloud Storage, Cryptographic Techniques for Data Security in Cloud Computing Cryptographic technique presents data integrity verification in Cloud Storage without using Trusted TPA (TTPA). TTPA is an independent component which is trusted by both cloud users and service provider. Three Level Security Systems for Dynamic Group in Cloud there is a need for more secure methods such as Image Based Authentication (IBA). After image authentication, user gets One Time Password (OTP).

The work in [2] surveyed critical security and privacy challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations, and envisioned future research directions and discuses Solution comparison and open research issues that include Encryption: Encryption can partially address the challenges associated with malicious insiders by preventing them from obtaining sensitive data and information in their readable format. However, encryption cannot be an ultimate solution to insider attacks since the insider may turn out to be a person who could legitimately decrypt the encrypted data or information, Access Control: By appropriately defining whether a user has the privilege to perform a given action on an object at a fine-grained level, access control schemes can be deployed by CSPs to effectively resist malicious insiders and DoS/DDoS attacks,Third Party Auditing: TPA is helpful with deterring malicious insider attacks. By auditing the activities of the employees, it is more probable for a security team to detect any suspicious activities indicating the existence of a malicious insider,Isolation: Isolation based schemes are mainly proposed to address security issues caused by multi-tenancy and virtualization,Soft Trust: The establishment of trust in the cloud could improve the detection of malicious behaviors, promote [7]collaborations among trustworthy parties and further facilitate the broad adoption of cloud computing technology,TPM can be effectively used to prevent insiders from performing different malicious activities such as gaining access to customers' confidential information or accessing the shared resources without proper authorization, etc.Governance: Governance solutions mainly address the managerial challenges in cloud security. However, all the technical solutions to the technology-centric cloud security challenges are also dependent on how well the technical countermeasures are managed in one way or another.

Another contribution is in [3] this paper includes the advantages and the disadvantages in the cloud computing and explain the security model of cloud computing, and then analyze the feasibility, threats, and security in cloud computing in terms of extensive existing methods to control them along with their pros and cons. After that, the related open research problems and challenges are explored to promote the development of Cloud computing,Privacy Challenge The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance [8]. As with security, it is necessary to design in privacy from the outset, and not just bolt on privacy mechanisms at a later stage,Information that needs protection:Personally identifiable information (PII)-

Sensitive information-Information considered being sensitive PII-Usage data-Unique device identities,Privacy risks for cloud computing: The main privacy risks are For the cloud service user,For the organization using the cloud service,For implementers of cloud platforms,For providers of applications on top of cloud platforms and For the data subject,key privacy requirement are Notice, openness and transparency,Choice, consent and control,Scope/minimization,Access and accuracy,Security safeguards,(Challenging) compliance,Limiting use – disclosure and retention and Accountability.

[4] in cloud computing many benefits: Availability of services and data is guaranteed, cost for consumption, ease of deployment, technical infrastructure adaptable to business volume, and suitability for common business applications (CRM, HR, BI, ERP, mail etc) This service provides a business function and not the technical components that require computer skills ... Besides these advantages [9], there is a high risk of using cloud computing, such as temporary or permanent loss of data, data security, lack of traceability and accountability ... these risks Are the main challenges Faced when adopting cloud computing architecture. In this paper, we have studied literature focusing on three key concepts about collaborative cloud computing systems: security, privacy and trust.

[5] an online study was conducted to measure user behavior towards data privacy and security in cloud-based systems. The research was conducted by offering an online survey of computer science students and employees of various software companies in the Netherlands and Macedonia.

[6] The centralization of sensitive health data in cloud computing raises many security and data-related issues. Given the importance and sensitive nature of health data, medical institutions are hesitant to transfer patients to the data in the cloud. This paper analyzes security and privacy issues raised by the use of cloud in e-health

III. SECURITY AND PRIVACY PROBLEM ISSUES OF CLOUD

It is main to insure that privacy is kept in all the situations. So, the work takes us in both paths: preserving the privacy of the data as well as preserving the privacy while we preferably some third-party auditing to confirm the data correctness.

A. Privacy Preserving Schemes

The important part of the providers is to preserve privacy of the consumer where their exclusive information is stored in the cloud. Due to scanty user control, information disclosure, uncontrolled data reproduction, [10] unauthorized second storage and dynamic provision there exists little issues that could drive cloud service providers to reach privacy. Different security problems and threats that impact the privacy preservation of the data users are analyzed. Also, the methodologies used to solve the security threats are analyzed. Different cryptographic mechanisms that are used to resolve the security threats are specified.

1. Public Key based Homomorphic Linear Authentication:

This scheme presents Public Auditing and Privacy Preserving for Data in Cloud. Data Security is a major issue inCloud computing that needs to be considered. The customer's data files stored in file server without keeping copy in the cloud because they cannot trust the clients and unreliable server.
The customers should be able to detect change in any part of client's data, if server modifies; furthermore, the third party auditor must also be able to detect it. Using Homomorphic Linear Authentication protocol provides privacy preserving data security with random masking. And hence, client can easily trust the service provided by cloud, as TPA works on behalf of cloud user. The data will be kept private against the third-party auditor.

2. Cryptographic Techniques for Data Security:

Cryptographic technique presents data integrity verification in Cloud Storage without using Trusted TPA. Trusted third party auditor (TPA) is an entity which is trusted by both consumer and provider. cryptographic algorithm includes two types of key: symmetric key andAsymmetric key for encryption and decryption of data. Algorithms such as RSA and DES are used for encrypting and decrypting data and then by using hash function hash code is generated. Data owner encrypts the file, generates signature using hash function and uploads to cloud. Whenever the owner wants to change data, a request is send to provider. Service provider generates hash code data for encrypted file, decrypts it and sends it to data user. Hash functions such as MD5, SHA1, SHA2 and SHA3 are used for data correction and integrity verification.

3. Three Level Security Systems for Dynamic Group in Cloud:

Several techniques are implemented to protect data against unauthorized access. Text passwords are not enough to solve unauthorized access. more secure methods needed such as Image Based Authentication (IBA). Time Password (OTP). Users use this password to access data. This assures high level data security. The aim of Image based authentication is to provide three levels of security. It is a complex study where images are used as passwords and implementation is done using 3 levels of security. In Level 1, Simple text -based password is imposed. In Level 2, Image Based Authentication is imposed and it aims to eliminate attacks such as

tempest attack, shoulder attack. In Level 3, the1. Security System generates a one-time password (numeric password) which will be valid only for that login session. This one time password will be sent to user through his/her email id.

4. Data Privacy using Dynamic Reconstruction of Metadata:

Metadata is segregated and put into the cloud. The segregated data are grouped as non-private, partially private and exclusively private depending on data sensitivity. Next step is called as table splitting where the tables are divided horizontally and vertically. This splitting ensures the database normalization. Final step is called as ephemeral referential consonance which involves reconstruction of metadata as and when required by the cloud.

B. Public Auditing Schemes

While maintaining data integrity, it is also important to ensure that data is kept private against TPA.

Few effective public auditing schemes are given below:

1. Public auditing using Key generation method:

When a third party holds the data, there is a potential lack of control and transparency. This scheme provides efficient privacy preserving and public auditing for data security in cloud computing. It allows TPA to audit various users' data simultaneously.

2. Public Auditing using Hash Message Authentication Code (HMAC) Algorithm:

This scheme ensures that TPA audits the data without making any changes or modification to it and hence data privacy is maintained even against TPA. Cloud data storage service has three components First component User (U) stores large amount of data in cloud. Second component Cloud Server (CS) manages data storage. Last component Third Party Auditor (TPA) works on behalf of user to access data from Cloud Service Provider (CSP). HMAC is a cryptographic hash function that involves concatenation of hash code, key and the message together.

3. Public Auditing using One Ring to Rule Them All (ORUTA):

It is common that data is not only placed on cloud but also shared among the many users. When two users of group exchange information, the identities of users would indicate which users in the group has highest valuable target than others. The proposed scheme solves this problem. Homomorphic authenticators are constructed using ring signatures so that TPA will be able to verify integrity users' data of a group without having to retrieve entire data. Also ensures that identity of user is kept private from TPA.

Periodic Sampling Audit Approach:

This scheme provides dynamic audit services for un-trusted and outsourced storage. It aims to reduce the computation costs of third party auditors and storage service providers. The proposed scheme mainly classified into three processes such as tag generation, periodic sampling audit and audit for dynamic operations.

C. Encryption

Encryption can partially address the challenges associated with malicious insiders by preventing them from obtaining sensitive data and information in their readable format. Encryption helps with the multi-tenancy and virtualization challenges since it provides additional protection against a potential attempt from a tenant to steal the data or information belonging to another tenant who may be residing on the same physical machine. The major limitation of encryption algorithms is the encryption overhead, especially the computational burden. This burden becomes even bigger when the data to be encrypted is more dynamic in nature. For example, a log file is constantly updated, which will require an additional number of encryption attempts compared to more static files.

D. Access Control

The limitations of access control schemes are twofold.

1. Fine-grained access control schemes may introduce high complexity that limits their scalability.

2. Access control architectures usually assume that the data owners and the data servers are in the same security domain, where the data servers are fully trusted to commit access control policies. One feasible solution is to ensure the fulfillment of data owners' access control policies through other solutions, such as encryption.

E.Third Party Auditing

is helpful with deterring malicious insider attacks. By auditing the

Activities of the employees, it is more probable for a security team to detect any suspicious

Activities indicating the existence of a malicious insider. Since auditing is typically done

After the fact, TPA may not be able to detect DoS attacks in real time. However, there is an

Emerging trend to automate the auditing process, and the detection of DoS attacks could be

One of the responsibilities of TPA, but the reporting of the attacks may still occur once they

Are over. TPA can improve the transparency of a CSP by demanding more information on various aspects security readiness. TPA can partially handle multi-tenancy and virtualization challenges by

helping to discover potential security breaches in the multi-tenancy and virtualization environments.
The major limitation of TPA is its after-the-fact nature which makes it incapable of detecting an anomaly and reacting to it in real time. Furthermore, there are some areas of TPA that have not been heavily studied. This indicates much room for growth in terms of research in these topics.

F. Isolation

Isolation based schemes are mainly proposed to address security issues caused by multi-tenancy and virtualization. By creating dedicated logical devices for each single tenant, the isolation-based schemes aim to ensure perfect isolation where one tenant's performance is not interfered with by other tenants running on the same physical hardware.

G. Soft Trust

The establishment of trust in the cloud. Could improve the detection of malicious behaviors, promote collaborations among trustworthy parties and further facilitate the broad adoption of cloud computing technology.

H. Hard Trust (TPM)

TPM serves as a physical device to measure trust indicators in open platforms. It is bundled with commodity hardware that provides great flexibility in addressing some common security issues in cloud computing. The success of cloud computing heavily depends on how comfortable the customers are in outsourcing their sensitive data, losing control, and relying on the CSP's security controls. The CSUs need assurances from CSPs before the actual migration. TPM can play a vital role in strengthening the customer's trust by providing strong assurances about the integrity of their data and the cloud infrastructure.

TPM can be effectively used to prevent insiders from performing different malicious activities such as gaining access to customers' confidential information or accessing the shared resources without proper authorization, etc. TPM can effectively protect both platform and information integrity in the multi-tenant environment through a remote authentication mechanism with hardware-based attestation capabilities. TPM is used as a primary security measure. TPM allows customers to remotely verify data integrity or perform remote attestation, which can overexpose the cloud infrastructure and provide valuable information to outsiders.

I. Governance

Governance solutions mainly address the managerial challenges in cloud security. However, all the technical solutions to the technology-centric cloud security challenges are also dependent on how well the technical countermeasures are managed in one way or another.
Access control is also heavily dependent on management. To develop an efficient access control list, it is crucial to first develop proper policies and identify what to protect. Prioritization is another important facet of access control since not every asset can be protected.
Different displacement levels can be set to separate a VM from its neighboring VMs. If the VMs are from different CSUs who specify strong isolation in the SLAs, it is necessary for CSPs to strive to set the isolation level of the VM to its maximum degree. However, human errors can still occur and misconfiguration is possible. Therefore, management is a main factor here, too.

IV. CONCLUSION

Cloud computing is an model provide service, application, storage, network and other resource Remotely, Cloud computing enables resources appears larger or smaller than it actual using virtualization layer, we discuss the cloud computing advantages such as reducing cost and processing time, improving performance, increasing flexibility and collaboration, we are exploring a lot of research articles that covered cloud computing service, advantage, disadvantage, security issues and techniques used to achieve privacy preserving in cloud computing such as HLA and cryptographic Techniques for Data Security in Cloud Computing, TPA checks the integrity of data.

V. REFERENCES

[1] "Privacy Preserving Issues and their Solutions in Cloud Computing: Survey"MTech(CSE), BMSCE, Bangalore, India. And Prof. Dept. of CSE, BMSCE, Bangalore, India

[2] "A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions" Yuhong Liu et al.

[3] "Security and Privacy in Cloud Computing: A Survey"Naixue Xiong is the corresponding author.

[4] "Security, privacy and trust in cloud computing: A comparative study"Meryeme Alouane and Hanan El Bakkali.

[5] "Cloud Storage Privacy and Security User Awareness: A Comparative Analysis between Dutch and Macedonian Users". Adriana Mijuskovic, South East European University,Tetovo, Macedonia Mexhid Ferati, Oslo and Akershus University College of Applied Sciences, Oslo,Norway.

[6] "Data security and privacy in E-health Cloud: Comparative study".

[7] Hanafy, I.M., Salama, A.A., Abdelfattah, M. and Wazery, Y., 2012. Security in Mant based on Pki using fuzzy function. IOSR Journal of Computer Engineering, 6(3), pp.54-60.

[8] Hanafy, I.M., Salama, A.A., Abdelfattah, M. and Wazery, Y.M., 2013. AIS Model For Botnet Detection In MANET Using Fuzzy Function. International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), 3(1), pp.95-102.

[9] Houssein, E.H. and Wazery, Y.M., Vortex Search Topology Control Algorithm for Wireless Sensor Networks.

[10] Y.M.Wazery Survey on Wireless Sensor Network Current Security issues, international journal for research & development in technology, Volume-6,Issue-5(Dec-16)