Data Security and Privacy Protection Issues in Cloud Computing

Dr.P.K.Rai¹, R.K.Bunkar², Vivekananda Mishra³
¹Computer Center, APS University Rewa, M.P., India.
²Computer Science, IGNOU Tribal University Amarkantak, M.P., India.
³Vindhya Institute of Technology Satna, M.P., India.

Abstract: It is accepted that cloud computing has many potential advantages and many activity applications and data are migrate to public or hybrid cloud. But concerning some business critical applications, the organizations, particularly large enterprise, still wouldn’t move them to cloud. The market size the cloud computing common is still far behind the one expected. From the client’s viewpoint, cloud computing security concern, specially data security and privacy protection issues, remains the primary restrain for adoption of cloud computing services. This paper provide a summarizing but all-around analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solution. Finally, this paper describes upcoming research work about data security and privacy safety issues in cloud.

Keywords: access control, cloud computing, cloud computing security, data segregation, data security, privacy protection.

I. INTRODUCTION

From initial concept building to current actual deployment, cloud computing is growing more and more mature. Nowadays many organizations, especially Small and Medium Business (SMB) enterprises, are increasingly realizing the benefits by putting their applications and data into the cloud. The acceptance of cloud computing may guide to gains in effectiveness and usefulness in developing, use and save the cost in purchasing and maintaining the infrastructure. A propos definition of cloud computing model, the most generally used one by NIST as “Cloud computing is a model for enabling flexible, on demand network entrance hall to a public pool of configurable computing material goods, (e.g., network, servers, storeroom, application, and services) that can be fast provisioned and free with minimum managing effort or overhaul source interaction. This cloud representation promotes ease of use and is collected of five essential features, three service model, and four use models[1]. Cloud Software support by Core Electronic Device High General Chip and Basic Software program of China: 2011ZX01043-001-001 Supported by National Natural Science Foundation of China: 60803131 Supported by Electronic Information Industry Development Fund Project: “Multi-industries oriented Information Technology Services Knowledge Base System growth” support by National basic research program of China (973):2012CB724107 Service (SaaS), (PaaS) and (IaaS) and four advance models are: Private, Community, Public and Hybrid cloud Compared with the established IT model, the cloud computing as many possible advantages. The clients’ viewpoint, cloud computing security concerns remain a major barrier for the adoption of cloud computing. According to a survey from IDC in 2009, 74% IT managers and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues [2]. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Protection incidents even lead to fall down of cloud computing vendors. As the administrator mistreat leading to loss of 45% user data, cloud storage vendor Linkup had been forced to close. Security organize measures in cloud are similar to ones in conventional IT environments. As multi-tenant characteristic, service delivery models and deploy models of cloud computing, compared with the traditional IT surroundings, however, cloud computing may face different risk and challenges.

Usual protection issues are still nearby in cloud computing environment. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in cloud. Due to the openness and multi-tenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field:

(1) Due to dynamic scalability, service abstraction, and location transparency features of cloud computing models, all kinds of applications and data on the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it’s difficult to isolate a particular physical resource that has a threat or has been compromised.
(2) According to service delivery model of cloud computing, services based on may be owned by several providers. There is a conflict of interest, it is difficult to deploy an integrated security measures.

(3) As the directness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by other unauthorized users.

(4) The cloud platform has to arrangement with considerable information storage and to deliver fast access, cloud security dealings have to meet the need of massive information processing. This term describe data security and privacy protection issues in cloud.

This manuscript is organized as follows: Section II gives a brief description of what exactly cloud computing security-related issues are. Section III discusses data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Section IV shows current solutions for data security and privacy protection issues in cloud. Section V summarizes the contents of this paper. Section VI describes future research work.

II. CLOUD COMPUTING SECURITY ISSUES

A. Cloud Computing Security

Wikipedia [3] define Cloud Computing security like “Cloud computing security referred to merely as "cloud security" is a developing sub domain of CPU safety, network protection, and, more largely, Information security. It refers to a wide set of policies, technologies, and gearshift deployed to care for data, application, and the linked infrastructure of cloud computing.

B. Protection Issues linked with the Cloud Computing

There are several security issues connected with cloud computing and they can be grouped into any number of dimensions. According Gartner’s [4] making a choice of cloud vendor, users should ask the vendors for seven particular safety issues: Privileged user access, regulatory compliance, data position, data separation, revival, investigative support and long term feasibility. In 2009, Forrester Research Inc.[5] evaluated protection and privacy practices of some of the leading cloud providers (such as Salesforce.com, Amazon, Google, and Microsoft) in three major aspects: safety and privacy, agreement, authorized and contractual issue. Cloud Security Alliance (CSA) [6] is get-together result provider, non-profits and persons to enter into discussion about the current and future best practices for information assurance in the cloud. The CSA has identified thirteen domains of concerns on cloud computing security [7].S.Sabatini and V. Kavitha made an investigation of cloud computing security issues from the cloud computing service delivery models (SPI model) and give a detailed analysis and assessment method description for each security issue [8]. Mohamed Al Morsy, John Grundy and Ingo Muller explore the cloud computing security issues from dissimilar viewpoint, including security issues related with cloud computing structural design, service deliverance model, cloud characteristics and cloud stakeholders [9].

Yampi Chen, Vern Paxton and Randy H.Katz believed that two aspects are to some amount new and necessary to cloud: the complexities of shared trust considerations, and the resultant need for mutual audit facility. They also place out small new opportunities in cloud computing security [10]. According to the SPI service delivery models, deployment models and essential characteristics of cloud, there are security issues in all aspects of the infrastructure including network plane, swarm level and purpose level.

![Cloud computing security architecture](image-url)
III. DATA SECURITY AND PRIVACY PROTECTION ISSUES

The substance of data security and privacy safety in cloud is similar to that of conventional data security and privacy protection. It is also implicated in every stage of the data life cycle. But because of directness and multi-tenant characteristic of the cloud computing, the substance of data security and privacy protection in cloud has its particularities.

The meaning adopt by Organization for Economic Cooperation and Development (OECD) [11] is any information relating to an identified or identifiable individual data subject. Another accepted definition provide by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard is “The rights and obligations of individuals and organizations with respect to the group, use, and disclosure of individual information”.

Data Life Cycle
Data life cycle refers to the entire process from generation to destruction of the data. The data life cycle is divided into seven stages. See the figure below:

![Data Life Cycle Diagram](image)

Figure 2. Data life cycle

A. Data Generation
Data generation is involved in the data ownership. In the traditional IT environment, usually users or organizations own and manage the data. But if data is to be migrated into cloud, it should be considered that how to maintain the data ownership. For personal private information, data owners are entitled to know what personal information being collected, and in some cases, to stop the collection and use of personal information.

B. Transfer
Within the venture boundaries, data broadcast usually does not require encryption, or just have a simple data encryption quantify. For data broadcast across enterprise borders, both data privacy and integrity should be ensured in order to prevent data from being tapped and tampered with by unauthorized users. In other words, only the data encryption is not enough.

Data integrity is also needed to be ensured. Therefore it should ensure that transport protocols provide both confidentiality and integrity. Confidentiality and integrity of data transmission need to ensure not only between enterprise storage and cloud storage but also between different cloud storage services. In other words, privacy and integrity of the whole transfer procedure of data should be ensured.

C. Use
For the static data using a simple storage service, such as Amazon S3, data encryption is feasible. However, for the static data used by cloud-based applications in PaaS or SaaS model, data encryption in many cases is not feasible because data encryption will lead to problems of indexing and query, the static data used by Cloud-based applications is generally not encrypted. Not only in cloud, but also in conventional IT environment, the data being treated is almost not encrypted for any program to arrangement with. Due to the multi-tenant feature of cloud computing models, the data being processed by cloud-based applications is stored together with the data of other users. Unencrypted data in the method is a grave threat to data security. Regarding the use of personal data, situations are more problematical.

The owners of private data need to focus on and ensure whether the use of personal information is consistent with the purposes of information collection and whether personal information is being shared with third parties, for example, cloud service providers.
D. Share

Data sharing is getting bigger the use range of the data and render data permissions additional complex. The data owners can permit the data admissance to one party, and in turn the party can more allocate the data to another party without the consent of the data owner. Therefore, during data sharing, especially when data shared with a third party, the data owner require to consider whether the third party continues to maintain the original protection measures and usage restrictions. Allotment of individual data, in addition to authorization of data, sharing granularity all the data or partial data and data transformation are also need to be concerned about. The sharing granularity depends on the sharing policy and the division granularity of content. The data transformation refers to isolating sensitive information from the original data. This procedure makes the data is not relevant with the facts owner.

E. Storage

The data in the cloud may be divided into:

1. The data in IaaS environment, such as Amazon's Simple storage space Service;
2. The data in PaaS or SaaS environment interconnected to cloud-based applications.

The data stored in the cloud storages is related with the ones stored in other sitting room and needs to reflect on three aspects of information security: confidentiality, integrity and availability. The familiar clarification for data privacy is data encryption. In order to ensure the effective of encryption, there needs to consider the use of together encryption algorithm and key strength. As the cloud computing environment involving large amounts of communication, storage space and usage, there also needs to consider processing speed and computational efficiency of encrypting large amount of data.

In this case, for example, symmetric encryption algorithm is more suitable than asymmetric encryption algorithm. One more key crisis concerning data encryption is key supervision. Is who responsible for key management? Ideally, it’s the facts owner. Other than at here, because the customers have not sufficient capability to supervise the keys, they generally hand over the key administration to the cloud providers. Cloud providers need to keep up keys for a large number of users; key managing will become more difficult and difficult. In addition to data privacy also needs to be troubled about data integrity. When the users put several GB or more data into the cloud storage, they how to check the reliability of the data? As swift smoothness characteristic of cloud computing property, the users don’t know where their data is being stored. To move around out of or into the cloud storage will consume the user’s network utilization (bandwidth) and an amount of time. Some cloud provider such as Amazon require users to pay transmit amount How to openly verify the integrity of data in cloud storeroom without having to first download the data and then upload the data is a great challenge. The data is active in cloud storeroom, the traditional technologies to guarantee data integrity may not be effective. In the traditional IT environment, the main threat of the data availability comes from external attacks. In the cloud, however, in addition to external attacks, there are several other areas that will threat the data availability:

1. The availability of cloud computing services;
2. Whether the cloud providers would continue to operate in the future?
3. Whether the cloud storage services provide backup?

F. Archival

Archiving for data focuses on the storage media, whether to provide offsite storage and storage duration. If the data is store on convenient media and then the media is out of control, the data are likely to take the risk of leakage. If the cloud service provider don’t provide offsite archiving, the availability of the data will be vulnerable. Again, whether storage duration is consistent with archival requirements? Otherwise, this may result in the availability or privacy threats.

G. Destruction

When the data is no longer required, whether it has been completely destroyed? Due to the physical characteristics of storage medium, the data deleted may still exist and can be restored. This may result in inadvertently disclose of sensitive information.

IV. Current Security Solutions For Data Security And Privacy Protection

IBM developed a fully homomorphism encryption scheme in June 2009. This scheme allows data to be processed without being decrypted [12]. Roy I and Ramada applied decentralized information flow control (DIFC) and differential privacy protection technology into data generation and calculation stages in cloud and put forth a privacy protection system called air vat [13]. This system can prevent privacy leakage without authorization in Map Reduce computing process. A key problem for data encryption solutions is key management. On the one hand, the users have not enough expertise to manage their keys.

www.irosjournals.org 42 | Page
On the other hand, the cloud service providers need to maintain a large number of user keys. The OASIS and Key Management Interoperability Protocol (KMIP) is trying to retort such issues [14]. About data integrity confirmation, the data communication, transfer fees and time cost, the users cannot first download data to verify its correctness and then upload the data. And as the data is dynamic in cloud storage, traditional data integrity solutions are no longer suitable. NEC Lab’s provable data integrity (PDI) solution can support public data integrity verification [15], Cong Wang proposed an arithmetical method to authenticate the integrity of the data dynamically store in the cloud [16]. In the data storage and use stages, Mow Bray proposed a client-based privacy management tool [17]. It provides a user-centric trust model to help users to control the storage and use of their sensitive information in the cloud. Muns-Mulero discussed the problems that existing privacy protection technologies such as K anonymous, Graph Anonymization, and data preprocessing methods faced when applied to large data and analyzed current solutions [18]. The challenge of data privacy is sharing data while protecting personal privacy information. Randike Gajanayake proposed privacy protection framework based on information accountability (IA) components [19]. The IA agent can identify the users who are accessing information and the types of information they use. When inappropriate misuse is detected, the agent defines a set of methods to hold the users accountable for misuse. About data destruction, U.S. Department of Defense (DoD) 5220.22- the National Industrial Security Program Operating Manual shows two approved methods of data devastation protection, but it does not provide any specific requirements for how these two methods are to be achieved [20]. The National Institute of Standards and Technology (NIST) Special journal [21], 800-88, gives a “Guidelines for Media Sanitization”.

V. CONCLUSION

Although cloud computing has many advantages, there are still many actual problems that need to be solved. According to a Gartner survey about cloud computing revenues, market size for Public and Hybrid cloud is $59 billion and it will reach USD 149B by 2014 with a compound annual growth rate[22]. The revenue estimation implies that cloud computing is a promising industry. But from another perspective, existing vulnerabilities in the cloud model will increase the threats from hackers. According to service delivery models, use models and essential features of the cloud computing, data protection and privacy security issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues exist in all levels in SPl service delivery models and in all stages of data life cycle. The challenges in privacy protection are sharing data while protecting personal information. The usual systems that require privacy protection are e-commerce systems that store credit cards and health care systems with fitness data. The ability to control what in order to reveal and who can access that in order over the Internet has become a on the increase fear. These concern consist of whether individual in categorize can be stored or read by third parties without authorization, or whether third parties can follow the web sites somebody has visited. One more apprehension is whether web sites which are visited collect, store, and probably share individual information about users. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements. Reading of data security and privacy protection issues above is estimated to have comprehensive security solution to meet the needs of defense in depth. Privacy protection, privacy data identification and isolation are the primary tasks. They should be considered during the design of cloud based applications.

VI. Future Work

The security issues and privacy protection is the main challenges and separation of aware of admission control. This papers objective is to propose a set of unified identity management and privacy protection frameworks across applications or cloud computing services. Employees in the organization is reasonably large, identity management system should achieve more usual and fast user account provisioning and de-provisioning in order to ensure no unauthorized access to organizations cloud resources by some employees who has left the organizations. Authorization and admittance control mechanism should accomplish a unified, reusable and scalable access control model and meet the need of fine-grained access permission. Responsibility based privacy precautions mechanisms will achieve dynamical and real time information, authorization and auditing for the data owners when their private data is being accessed.

REFERENCES


www. iosrjournals. org 43 | Page


