International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

CDSM : Wide-Ranging Cloud Data Security Management System

M.Thanmayee, Vasavi Sravanthi Balusa
Assistant Professor, Department of Computer Science and Engineering, TKR College of Engineering and Technology, Hyderabad, Telangana, India

ABSTRACT

Cloud computing is a service model in which the computing resources such as software, hardware and data are delivered as a service through a web browser or lightweight desktop machine over the internet. Cloud computing has increased its acceptance in recent years. Despite of having a number of benefits, users are still worried about security of data in cloud due to losing the control of their own data when outsourced in cloud environment. The security is an important feature in all sorts of Information systems, the cloud computing is no exception. The confidentiality, integrity and availability are the key issues affecting security of data in cloud along with dependability of users and cloud service providers. There are increasing security and privacy concerns from the point of view of both the enterprises and the individuals of their outsourced data in cloud. Several security management standards and measures have been intended to security the cloud but still cloud security is at a high risk due to the pioneering hacking techniques. In this paper we propose wide-ranging data security framework for cloud computing for the designing of security framework called CDSM system. The cloud data security management framework is proposed for providing Information Security as a Service (ISaaS). The framework ensure the security of data during rest in cloud, and when data in flight between different entity of cloud system. The CDSM framework provides a flexible and modified data storage, computation, backup and disaster data management service which can be expanded and altered according to the needs of the organizations and users.

Keywords : Cloud Computing, CDSM, integrity and availability.

I. INTRODUCTION

The cloud computing is a new concept for delivering computing service and largely satisfies emerging requirements of the information technology. It has claimed itself to be of great benefit for users and organizations because it can dramatically reduce the expenses and provide an aid to manage information technology systems without any hassle [1]. Due to its large number of advantages, Cloud has been increasingly adopted in many areas, such as banking, e-commerce, retail industry, and academics etc. In addition to it [2, 3] cloud computing also reduces the risk of capital expenditure for IT companies. On the other hand, cloud vendors can deliver more efficient management and coordination of cloud resources to achieve profit optimization and maximization. Subashini and Kavitha [4] suggest that small and medium size companies can also use cloud computing services for various reasons, as these services provide fast access to their computing resources, applications and reduce infrastructure costs. However, the cloud alters the traditional service rules of data computing service management. Now, in cloud data management services are operated in the customers' local environment but are remotely served by cloud service providers (CSPs). Although this segment demonstrates a number of potential advantages

compared with the conventional computing systems, such as providing infinite data storage capability, high-performance services with low cost, interactive data sharing. However, on the other hand, users are concerned about losing control of their own data [5]. In terms of an important characteristic of cloud computing, resources and services are offered to the users in an abstract form. Users may not know where, when, how, why, and by whom their data is accessed or modified in cloud environment [6, 7]. However, cloud computing suffers from many security issues[8]. Moreover, CSPs are more vulnerable to adversaries or hackers who may exploit to gain the benefits. The cloud is vulnerable in respect of data security, privacy, and confidentiality as users' sensitive data is stored in a third-party CSP. The encryption [9] of data can merely resolve confidentiality and integrity challenges, but to adopt cloud largely, establishment of a trustworthy relationship between the cloud providers and the users is necessary.

II. Background

The cloud computing is a service model which was actually introduced to render computational resources over the internet and it has been accepted and used by the industry also in addition to user. But still there are many open challenges which needs to be address so that it can fully adopted by the industry and to make this model more secure, efficient, and cost effective for user's requirements [12-13]. Despite the initial success and popularity of the cloud computing paradigm and the extensive availability of providers and tools a significant number of challenges and risks are inherent to this new model of computing. The service providers, developers and end users must consider these challenges and risks for wide adoption and take advantage of cloud computing. The challenges and risks include data security and privacy, data lock-in and availability of service, disaster recovery, performance, scalability, energy-efficiency, and programmability, interoperability.

Data Security and Privacy

The end users of cloud services are have serious concerns about the confidentiality, integrity and availability (CIA) of their data that has been outsourced to the cloud [12]. The researcher mentioned that advantages of cloud are shadowed with data security, safety, privacy and anonymous challenges in [8, 82]. Data needs to be protected from unauthorized access while maintaining the integrity of user' data. So the challenge that arises is to develop secure and efficient system to maintaining confidentiality and integrity of data in cloud.

Data lock-in and Standardization

The data lock-in and standardization is a major concern that need to be dealt with in cloud computing. Users may want to move data and applications out from a provider that does not meet their requirements. However, in their current form, cloud computing infrastructures and platforms do not employ standard methods of storing user data and applications. Consequently, the data is not interoperable with other providers and user data is not portable. The answer to this concern is standardization. For this efforts have been made to develop open standards for cloud computing

Availability and Disaster Recovery

It is expected that users will have certain expectations about the service level to be provided once their applications are moved to cloud. These expectations include availability of the service, its overall performance, as well as what measures are to be taken when something goes wrong with the system or its components [14]. The SLA specifies the details of the service to be provided, including availability and assured performance. Additionally, SLA parameters must be agreed upon by all the parties involve as well as there are penalties for violation of these. Even if the user does not know where his data is, a cloud provider should tell to his user what will happen to data and services in case of a disaster. If CSP does not replicate the data and application in cloud infrastructure across multiple

data centre then the data is prone to a complete failure of service [17].

III. Problem Statement

Data privacy is the significant factor for the achievement of the cloud technology. In many reviews and researchers, it is revealed that security is now the core challenge to be compact in the cloud. It has presented itself many of the cloud computing security issues which are similar to the traditional ways of in-house computing in a new way. This requires re-assessing the risks related to each of the critical areas in the new hazardous environment, where the resources are shared by multiple users as discussed in. Depending on the cloud model which user use the level of multi-tenancy and security issues would be different. But without any reservation, Infrastructure-as-a-Service (IaaS) of public cloud, risks highest amongst all. Several security management standards and measures have been intended to safeguard the cloud system, but its security is at high risk due to the innovative hacking techniques. This work focuses on identifying the security threats and issues and their countermeasures to strengthen the confidentiality, integrity and availability (CIA) of data stored cloud. This work proposes a wide-ranging data security solution, and protocols to efficiently address the security and privacy-related risks inherent in cloud computing that represents itself as a complex and challenging. Also, focus on privacy and security of data outsourced in the cloud and provide secure cloud-based storage and computation service, to address issues related to maintaining the confidentiality of data during transfer between different entities in the system, and during their stay in the cloud system, to protect data from malicious insiders and outsiders. These issues shall refer "The Cloud Security Management Problem."

1. Objectives Of Research Work

The primary aim of this research is to propose comprehensive information security framework for IaaS model of cloud computing. There is a need to design and develop a **cloud data security management system (CDSM) to** improve security and privacy of data outsourced to the cloud. The framework shall provide information security as a service (ISaaS) to the cloud service.

Specific Objectives to be design to improve the data security in cloud computing is as follows:

Objective– To Design and implement an effective secure access control management system (SACM)

That is an essential part of the proposed comprehensive security framework. The SACM system is going to implements a set of protocols to provide secure authentication and authorization as a service (SAAaaS) to users in the cloud system. Also, address the issue related to unauthorized access to cloud computing resources. Indeed, it is required to propose an efficient and robust user registration, authentication, and authorization and user management mechanism further.

2. Proposed model

This proposed model and methodology is based on a comprehensive software engineering approach, it is going to include a historical analysis of threats and attacks in cloud computing as well as countermeasures within the context of security domains. It is recognized the requirements and proposes a system that meets the needs. Then implement a prototype according to the design of the proposed security system. To analyses feasibility and validation proposed system runs for using some test case for evaluation of results and performance, is refined and designed to achieve better research outcomes.

3. Architecture of Cloud Security Framework

The proposed security system has three stockholders that are:

(i) Cloud service provider (CPS) which provides cloud resource (storage and computing);

(ii) Middleware cloud data security system CDSM and;

(iii) Cloud service consumers (CSC).

The CDSM implement security policy and functionality for data security. The cloud service consumer/user uses the cloud services for their computing needs. The user access cloud services that provided by CSP, through the proposed security framework CDSM. The Fig. 1 shows illustrative representation of the proposed security framework along with its functional constituents. The CDSM system act as a security gatekeeper/gateways that ensure the secure access to cloud service and data that are outsourced and provided by untrusted cloud service provider. The CDSM is a middleware system between users and CSP that implement information security protocols. The CDSM server is responsible for provided efficient, flexible, fine-grained access control for cloud resources (storage and computing). It provides authentication and authorization service, database management, user management, cryptography service and also ensures the confidentiality, integrity and availability of data in cloud. The CDSM system provides centralized security solution for cloud based services and delivered Information Security as a Service (ISaaS) from untrusted public cloud. It ensure multi-dimensional security of data to increase the security posture for IaaS model of cloud computing. The service oriented architecture of the CdSM is shown in Fig. 1 has four well-defined functional module or subsystem. These are (i) secure access control management system (SACM);

(iv) privacy-preserving data storage management system (PPDSM)

(v) privacy-preserving data computation management system (PPDCM) and;

(vi) Efficient data Backup and Disaster Recovery Management system (BDRM). The system allows the administrator to define security policies, efficient management of system to provide uninterrupted cloud services to the users. The function of administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and performing backup and recovery tasks. The detailed construction of each component of proposed system is described here:

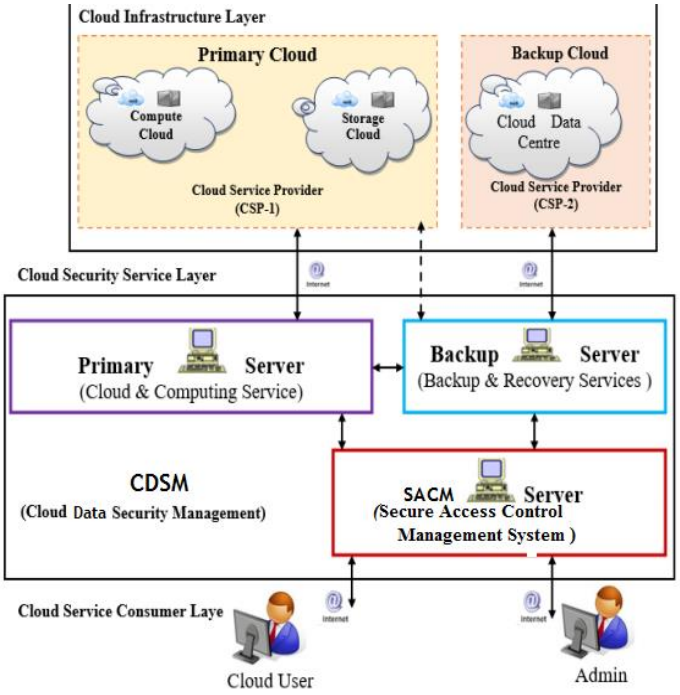

Figure 1. Proposed security framework

Cloud Infrastructure Layer:

This layer is formed by different CSPs, which are hosting cloud computing resources in their large data center and delivered computing service to the user over the internet through security CISM system. These cloud services and resources are available to users over the internet through security framework CISM. In the backend cloud computing resources and services are provided by cloud service provider that is called primary CSP and backup CSP. As shown in Fig. 1 the primary cloud service providers (primary CSP) provides data storage (storage cloud)

and for data computation (compute cloud) resources. Similarly backup CSP provides for data backup in addition to primary cloud. The backup cloud (CSP) host additional computing resource that are used to deliver services in case of disaster in cloud system. The computing and storage resources and data of backup CSP is used when primary CSP is out of function and data are not available due to disaster. The users' data is stored into backup CSP in accordance with the threats arising and the security policy according to the security policies. The primary cloud (CSP-1) is associated with primary server (PS) and backup server (BS) of security framework CISM. Similarly backup cloud (CSP-2) is associated with backup server (BS). The Infrastructure as a Service (IaaS) and cloud computing services are provided by the primary and backup cloud which is operated in cloud infrastructure layer of proposed security framework CISM. The primary and backup cloud provides cloud resources for storage and computation services, from their large datacenter. These computing resources are provided to the user on-demand over the internet anytime, anywhere manner through a middleware system i.e. CISM. The SLA, QoS and security criteria for cloud services are different according to the service level agreement mentioned during the negotiation process and are predefined. Due to the limited resource the proposed security framework was simulate only for cloud storage services using Dropbox. The virtual datacenter is created using application developer tools provided by dropbox cloud service providers.

Cloud Security Service Layer (Cloud SSL)

The cloud security service layer is formed by proposed security framework CISM system. In this layer three security servers primary server(PS), backup server(BS), IAM server are implements security policies and mechanism to ensure data security in Cloud. The primary server implements the secure data storage and computation management services. The primary is associate with one cloud service providers called primary CSP, which provides data storage and computation service to the users. The user interact with CISM system using his local machine (PC or smart phone), secure internet connection, and user interface. The CISM server acts as a gateway to access cloud resources provided by cloud service providers (CSP) for their computing requirements. The user first interacts with IAM server of CISM system to access cloud service (resources) provided by the different cloud service provider (Primary CSP or Backup CSP) associated with this system. The hackers are also attack in this layer primarily to get deeper access into the cloud system, due to this it is extremely important how this layer is secured.

The cloud security service of the CISM system is implemented as shown in Fig. 1. In proposed security framework CISM, a primary cloud service provider (CSP) which is hosting huge cloud resource for computation and storage service in large data (Primary Cloud) and a backup cloud service provider (Backup CSP) hosting cloud resource for backup service. The primary servers and backup server have identical functionally and but having different resource capacity. However the primary server deliver services to the users for primary storage and computation purpose, while the backup server deliver data backup service when primary system is not functioning in due to disaster. The backup server is used to store data for backup and implements business continuity and recovery policies.

Cloud Service Consumers Layer

The cloud service consumer layer is formed by cloud service consumers also called users that are registered with CISM system for their computing needs. Only authorized user of the CISM system is allowed to access cloud services. The cloud service user accesses the cloud services and resources provided by CISM through local computer called client machine. The client-side cryptographic tools are installed on client machine that used for encryption (pre-processing) and decryption (postprocessing) of data to be outsourced into cloud resources (storage and computing). These cloud resources and services are

accessed by the user using client machine (PC, smart phone). The secure internet connection, web browser, and secure interface which are the access point for the cloud services. The hackers also attacks in this layer at primarily to get deeper into the cloud structure. These access points are very sensitive and vulnerable for security threats. It is extremely important that this layer is to be secured enough. As shown in Fig.1 the large number of cloud service users request for cloud services, access cloud service for their computing needs that are provided by the cloud service providers (CSP) from their large data center. The cloud service user access cloud resource through primary and backup server of proposed security framework CISM. In this layer each user has its own client machine (CM) with low computing power. The client machine is installed with cryptographic tools provided by CISM system, for encryption and decryption of data. These encryption tools are used for encryption of user data before outsourced to the cloud. The cloud user establishes a secure connection with CISM server.

Test Case Analysis

The users are classified into three classes are honest, malicious and random according their behavior over long time interaction with system which are describe as below:

- Honest users: The user whose behavior is positive for most of the time (90 % approximately) due to more authorized activities and sometime (10 % approximately) due unauthorized activities.
- Malicious user: The user whose behavior is negative most of the time (90 % approximately) due more unauthorized activities and very less (10 % approximately) authorized legal and positive activities.
- Random user: The user whose behavior is positive or negative due authorized and unauthorized activities randomly. It is further assumed that positive (60% approx.) activities are more than negative (40% approx.) activities. The performance parameter to calculate trust value of user is:
- Uncertainty- It shows the uncertainty in user behavior and trustworthy it have initial value is 1 show highly uncertainty in about new user behavior. As user has more interaction it becomes 0 which shows the certainty in user behavior that may honest, malicious or random.
- Degree of Trust (DoT): It represents degree of trustworthiness (trust value) of user, and its value increase or decrease depending credential and behavior trust of user.
- Behavior Trust (BT): It represents the behavior trust of user, and which depend on Up trust or Down trust, due positive and negative behavior of user respectively.
- UpTrust : Represents positive trust value due to the positive behavior of user
- DownTrust: Represents negative trust value due the negative behavior of user.

IV. Conclusion

In this paper we propose wide-ranging data security framework for cloud computing for the designing of security framework called CDSM system. The cloud data security management framework is proposed for providing Information Security as a Service (ISaaS). The framework ensure the security of data during rest in cloud, and when data in flight between different entity of cloud system. The CDSM framework provides a flexible and modified data storage, computation, backup and disaster data management service which can be expanded and altered according to the needs of the organizations and users.

V. REFERENCES

[1]. W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to Cloud Computing," in Cloud Computing, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011, pp. 1-41.

[2]. T. S. Mohan, "Migrating into a Cloud," in Cloud Computing, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011, pp. 43-56.

[3]. M. A. Vouk, "Cloud Computing Issues, Research and Implementations," Journal of

Computing and Information Technology, 2008, vol. 16, no. 4, pp. 235-246.

[4]. S. Subashini and K. Veeraruna, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 1-11.

[5]. J. Wang and S. Mu, "Security issues and countermeasures in cloud computing," in Proceedings of IEEE International Conference on Grey Systems and Intelligent Services, 2011, pp. 843-846.

[6]. K. Gai and S. Li, "Towards Cloud Computing: A Literature Review on Cloud Computing and Its Development Trends," in Fourth International Conference on Multimedia Information Networking and Security, 2012, pp. 142-146.

[7]. R. K. L. Ko, M. Kirchberg, and B. S. Lee, "From system-centric to data-centric logging - Accountability, trust and security in cloud computing," in Defense Science Research Conference and Expo (DSR), 2011, pp. 1-4.

[8]. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, 2010, vol. 8, no. 6, pp. 24-31.

[9]. F. Zhao, C. Li, and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," in 16th International Conference on Advanced Communication Technology, 2014, pp. 485-488.

[10]. R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services," in Lecture Notes in Computer Science, 2010, vol. 6081, no. 1, pp. 13-31.

[11]. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific cloud computing: Early definition and experience," in Proceedings - 10th IEEE International Conference on High Performance Computing and Communications, 2008, pp. 825-830.

[12]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," EECS, Department, University of California, Berkeley, 2009, pp. 1-25.

[13]. B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, "Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, 2009, vol. 13, no. 5, pp. 14-22.

[14]. S. Mustafa, B. Nazir, A. Hayat, A. Rehman Khan, and S. A. Madani, "Resource management in cloud computing: Taxonomy, prospects, and challenges," Computers and Electrical Engineering, 2015, vol. 47, no. 1, pp. 5-13.

[15]. W. Wongthai, F. Rocha, and A. Van Moorsel, "Logging solutions to mitigate risks associated with threats in infrastructure as a service cloud," in Proceedings - International Conference on Cloud Computing and Big Data, 2013, pp. 163-170.

[16]. A. Abuhussein, H. Bedi, and S. Shiva, "Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing," in IEEE Sixth International Conference on Cloud Computing, 2013, pp. 958-959.

[17]. Q. Jiang, J. Ma, and F. Wei, "On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," IEEE Systems Journal, 2016, vol. 99, no. 1, pp. 1-4.