Volume 7, Issue 3, March 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security and Privacy in Cloud Computing with Vision Trends and Challenges

Sanjay Kumar*, Ram Singar Verma
Department of CSE, BBAU Lucknow, Uttar Pradesh,
India

Abstract— Cloud computing provides organizations and individuals with a cost-effective utility, empowering businesses by delivering software and services over the Internet to a large user base. Cloud computing is a distributed technology that compute on the basis of services such as the internet on demand and pay per uses access to a group of shared resources namely storage, servers, networks, services and applications etc. So it saves time and cost for managing organizations. Limited control over the data may invite various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and insider attacks. Cloud computing have adopted various types of challenges such as reliability, access control, privacy control, service level agreement (SLA) and interoperability. This paper summaries that what actually the cloud computing, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This paper explores the challenges, solutions, and limitations of cloud security, with a focus on data security aspects.

Keywords— cloud computing; services; cost-effective; organization; resources.

I. INTRODUCTION

Security of data storage, information usage administration get to control administration and trust are the significant security worry in distributed computing. Cryptography is the best way to deal with enhances the security in distributed computing. Conventional cryptography system is not generally utilized as a part of distributed computing as a result of restriction in computational efficiencies. . Homomorphic encryption has demonstrated that of give abnormal state of security yet it has some restriction since it require long calculation so we require more effective and versatile security arrangement with respect to distributed computing. Distributed computing models designated in information and application control so the customary strategies are not adequate to short out the issue that is the reason it has number of difficulties Unwavering quality is the major basic part of cloud administration reliability in cloud condition a trusted outsider and cryptographic techniques used to guarantee the credibility, trustworthiness and secrecy of both information and correspondence.

Client validation and information confirmation are associated in distributed computing. One of the significant issue of distributed computing is to shielding a client account from abuses of cloud based assets, (for example, memory, question, programming and devices).cryptography validation technique can ensure asset usage in distributed computing model ,key administration (denial ,conveyance and task) must be sensible and effective everywhere scale. Cloud is the new emerging technology in the evolution of the distributed systems, the predecessor of cloud being the grid. The user doesn't require knowledge about to control the infrastructure of clouds; it provides only abstraction. It can be utilize as a service of an Internet with high throughput, higher scalability, quality of service and high computing power.

II. CLOUD COMPUTING BUILDING BLOCKS

Mainly cloud services can be divided into three different categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

A. Software-as-a-Service (SaaS):

SaaS can be described as a process in which Application Service Provider (ASP) provide different software applications to the user. This makes the customer to free from burden of installing and operating the application on own computer and also eliminates the dreadful load of software maintenance; continuing operation, safeguarding and support [3]. SaaS vendor intentionally takes responsibility for preparing and managing the IT infrastructure (servers, operating system software, databases, data center space, network access and poweretc.) and processes (infrastructure upgrades, application upgrades, taking backups, etc.) required to run and manage the full solution. SaaS provides a complete application offered as a service on demand. There is different example of SaaS such as Workday, Concur, and Citrix GoToMeeting

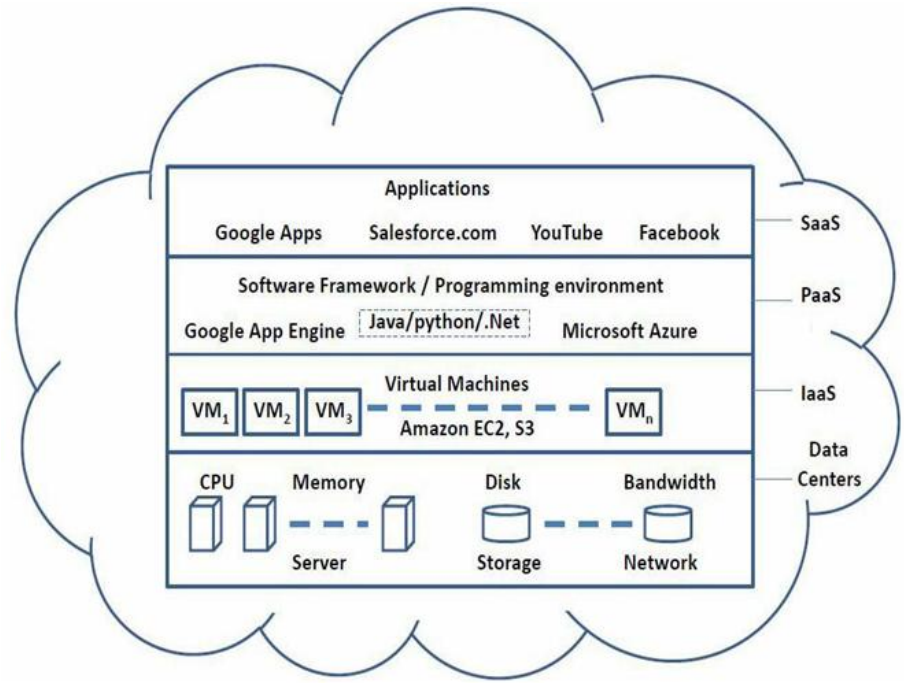

Fig.: 1 High Level View of Cloud Computing Architecture

B. Platform as a Service (PaaS):

Platform as serve can define as it is high level integrated environment in which customer created and test the applications. PaaS is extremely different from the SaaS because it's not simply use the application but it control the application and develop the application in hosting environment. PaaS mainly focus on the facilitating application development and its related management issues. Some service providers provides a general development environment and few of them provides only security and on demand scalability. Some of few examples of PaaS are Google app engine, MTark, engine Yard, Force.com, and Heroku etc.

C. Infrastructure as a Service (IaaS):

Infrastructure as a service is provides whole infrastructure to the user such as storage, processing, network, and other computing resources. IaaS is form of cloud computing so it is basically provides the virtual computing resources to the user over the internet. It contains all characteristic of SaaS and PaaS which mean we can access all application as per need and develop application. So IaaS provides a virtual third party infrastructure which contains all resources of high level computing infrastructure. It also provides the backup and maintenance facility to the users. It provides the resources with high scalable computing and can be change on demand, so we can adjust our infrastructure as per needed that's why it is most suitable for workload. It is working on the basis of pay per uses as hourly weekly and monthly. Leading company of IaaS services are amazon web service, Rackspace, IBM, GOOGLE Computing Engine.

III. DEPLOYMENT MODEL

There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

A. Private cloud:

It is a private cloud benefit where client or foundations have a private cloud to get to the administrations and have all control. So as indicated by the IT division each cloud must have security approach in which private cloud is secured by the firewall that will offer assurance to the private cloud. Private cloud give get to authorization to the approved clients, so the clients have consent to get to possess information and control over it , no other individual can't cooperate with that administrations. So it utilizes the better security strategies as contrast with the general population cloud that why we can state that it is a secured figuring model. There is critical variety in private cloud since it characterized by the administrations so it is hard to clarify. It might be inclined to helpless if there should be an occurrence of catastrophic event and insider assault however in different ways it much secures then open cloud. One of the best examples of a private cloud is Eucalyptus Systems [4].

B. Public Cloud:

Open cloud is the distributed computing model where seller has all authorization to do the assignment and controlling of cloud framework. End clients don't have authorization to control the cloud foundation. It is an open model where general client and diverse association can get to it, since it has share processing foundation. Open cloud is most reasonable for business necessities since it is a practical model that has less capital overhead and operational cost. The merchant gives the administrations as a free or some merchant have approach like pay per client. Example of free public cloud is Google.

C. Hybrid Cloud:

Hybrid cloud is the cloud infrastructure in which it included at least two cloud frameworks. In other word it is a mix of at least two cloud foundation such private and open cloud, so it contain the all properties of both the cloud framework. The workloads of half and half distributed computing depend on operational, cost and consistence variables. Some significant cases of cross breed framework are HP, Oracle, IBM AND VMware in which these organizations have intend to conveyed administrations to the business. Clients can get to the application benefit which is facilitated in the half and half cloud foundation, in which some procedure dealing with virtual condition and some taking a shot at physical equipment.

D. Community Cloud:

It is a kind of facilitating framework in which the setup is imparted to numerous associations that fundamentally have a place with a similar group, i.e. exchanging firm, saving money framework and so on it's a multi-tenant administrations or setup that common to the distinctive associations that has a place with the particular gathering which has same processing anxieties. The people group which has a place with a similar class shared same execution, protection and security issues. The principle part of these groups is to accomplish business related destinations. This kind of cloud administrations oversaw by inside or it can be overseen by the outsider give. So we can state that group cloud is the financially savvy foundation since association shared the assets so the cost of the administrations similarly appropriated. These mists are ordinarily in light of an understanding between related business associations, for example, keeping money or instructive associations. A cloud domain working as per this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in figure 1.

IV. CHALLENGES AND ISSUES

Unwavering quality of distributed computing is fundamentally relies on upon implementation of security strategies, (for example, information encryption, get to control) and security shortcoming must be tended to. Secure distributed computing present specialized, lawful and managerial difficulties. Fundamentally principle concentrate here is on the specialized issues. The primary motivation behind security uprightness, secrecy and accessibility must be tended to at the customer side, the association and server side. The significant issue is that all of three are work in shared condition so their security and protection prerequisite must join. The significance of cloud security has been broadly recognized, and a few associations have been taking a gander at it from alternate points of view.

A. Server Availability

Have essentially requires high accessibility on account of new innovation advancement, yet arrange get to be bottleneck. Information trade can be moderate in occupied system and could be possibility of assault on a system all things considered refusal of administration assault could be hurtful in light of the fact that it can hinder the essential assets. The stateless way of conventions require new answers for keep up the accessibility levels when we utilizing the web.

B. Data Storage:

One of client's real concerns is that how to store information safely. Clients don't know about information where really it put away so client dependably has some security question on specialist co-op. It is not unmistakably disclosed to the customer that how the information is secured on the server side. Information maintenance is additionally sympathy toward clients. The cloud specialist organization may keep record of erased information inbackup's reason however it could be abused for illicit reason. For instance, twitter and Facebook kept erased information however expelled it from view. Similar concerns likewise connected on clients when an administration is ended and information spared into the cloud.

C. Access Control:

Generally Most of the cloud environment includes the access control over the system. Generally administrator is included in every computing system that has all permission to access the user data. When data is outsourced using the cloud, then all data are handled by the safekeeping, and user don’t have knowledge about the actual data that mean user are unknown from its data location. The person (administrator) have permission to access the data so it could be chance attack that’s why it is also major security issue in cloud computing. So we can say that Insider threats or malicious employees are the main security concern in cloud computing. Malicious employees can be a reason for major harm, but outside attacker is also a biggest security issue in cloud computing. A privacy leak could be a reason for biggest harm because it could have person information and attacker revealed these information to the publicly. In some cases, data or processes are provided for a particular purpose, or stored with a particular aim in mind. A common concern is usage creep, when data stored in the cloud is accessed and used by the cloud service provider for a purpose other than the one the client intended. Cryptographic access control models address some of these issues. [6][7].

D. Identity protection:

Data traveling provides valuable information of the people over the internet. An anonymous can uses the some Search keywords such as, mobility patterns, and credit card usage that use to identify and track individual information, and then an attacker can reveal the personal information. Attacker can also track some information of the user interest

and then could be facilitated targeted advertisement and marketing. Data mining provide service that could not break the information of the client privacy if performed probably, it require the attention of the client that have some knowledge about it.

E. Multitenant storage:

Tenants are not generally isolated from each other in any shared service. There are many cloud server provide different levels of cloud services and uses the virtualization concept to separate clients, which includes allocating a virtual machine to a single user. If people work on same service then work pattern of one user can affect to other person. Such as one of the common problem is locking of resources that impacts on service availability consumer work in heterogeneous environments and the cloud service provider has excite on their setup. Some end users uses the service in a well-protected environment and some uses the service in less firewall protection so one user activity can affect to the other user work and servers due to which it could be possible that a malware can spread into the server and harm to the application and move to the other client. Virtual environment provide better security solution but still not complete isolation.

V. SECURITY IN CLOUD COMPUTING

A. Securing the Cloud with Homomorphic Encryption:

Data protection is the major concern of cloud users once the data has moved to the cloud. Customers need assurance of data that is well protected by cloud service providers. Encryption can mitigate this fear, but it has some drawbacks. The cloud provider can perform operations in the cloud to avoid time-consuming downloading and uploading of data for customers. Users must share their encryption/decryption keys with the cloud provider, effectively allowing them access to the data to manipulate encrypted data in the cloud. Homomorphic encoding permits computations may be administered on the idea of encoding and decoding of information, therefore generating Associate in nursing encrypted result, which, once decrypts, matches the results of constant operations performed on the initial information (plaintext). This can be a main advantage for applications in cloud computing.

B. Privacy preserving Data Mining as a service in the cloud:

For a decade, the interest in data mining as a service is growing. A company has lacks of data storage, computational resources stores and expertise in the cloud and out sources the mining tasks to the cloud service provider (server) [7, 8]. Data mining offers a valuable benefit to business intelligence. But it also has a serious privacy problem that is; the server has permission to access the company data and could learn business secrets from it. The server is to perform association rule mining on the data in the cloud to protect a company's data privacy, one of the best solution is to protect the data by the owner they must hide the meanings of items in its transaction database by substituting items with unique numbers (where the same item is substituted by the same number and different items are substituted by different numbers). This one-to-one substitution approach has some cons it doesn't hide the frequencies of items. If the server has some background knowledge then it can re-identify them, particularly the most frequent items such as, also important because these provide better services to mobile users by utilizing cloud resources. These mobile applications models use the services of the cloud to increase the capability of a mobile device. To prevent background-knowledge-based attacks, Wai Kit Wong and his colleagues proposed aone-to-*n* item mapping that transforms transactions non-deterministically [9].

C. Access Control in Cloud Systems:

Cloud computing generally offers cost-effective scalable platforms to provide different services to consumers or end users such as data analytics and data storage. The security of hosted or outsourced data is essential to ensure reliable service delivery in cloud systems. Data utilization management requires sufficient user authentications, authorizations, and scalable access control models. The access control models should essentially be secure and offer the required fine-grained authorizations along with efficiency to cater to a large user base.

D. Efficiency, Scalability, and Fine-Grained Solutions:

Access control is important security requirement to host sensitive data. One of the secure solutions for cloud system is cryptographic access control model. Fine-grained access control models can be developed by the combination some cryptographic techniques such as proxy re-encryption, lazy re-encryption hierarchical identity-based encryption, attribute-based encryption and cipher text policy attribute-based encryption for cloud systems.[10],[11]. The use of cryptographic techniques incurs heavy computational overheads on the data owner for both key distribution and data management tasks. For example, when adding or deleting users from the system, tasks include revoking keys, updating keys of other users, and re-encrypting data. Further improving scalability and efficiency while providing fine-grained authorizations requires advanced cryptographic access control models. Advanced models have been developed using a combination of cryptographic techniques with efficiency and security guarantees.

E. Distributed Access Control:

One of the silent features of the cloud deployment model is decentralization administration. Decentralization access control is desirable in cloud environment because in centralized solutions, access control for a large number of users over multiple clouds is very complex. Solutions of that problem is multi authority cryptographic access control

models.[14] However, it's important to consider the application-specific requirements along with multi-tenancy and the distributed nature of cloud-based deployments in developing more scalable access control models.

F. Access Control as a Value-Added-Service

The lack of access control create difficulties or make effect on working of data sharing applications in cloud computing. For cloud-based utility service models, offering access control as a value added service is more pragmatic. [15] So it requires sufficient secure utility model. Overlay service given the sufficient solution of the access delay. For example, researchers have given a self-maintained quorum of key managers to handle the cryptographic key operations for fine-grained policy-based access control. [4]Trusted key managers are required to ensure sufficient security in access control.

G. Reliable Credential Management:

Robust authentication is vital in access control: authorizations are granted to authenticated users. An important aspect of this is the management of identity credentials. Federated identity management is deemed an efficient solution for open systems such as cloud-based collaborative systems. Trustworthy identity management is essential to ensure reliable data utilization management. Useful trust evaluation metrics are proposed to estimate the reliability of security, and to be offered as a cloud utility service. [16]The significance of trust evaluation is vital to ensure secure collaborative data sharing, data analytics, and data outsourcing.

VI. CONCLUSION

Cloud computing is one of emerging technology trends in the future since it containing many advantages but one of the most concerns among the researcher is security. This paper mainly focus the security of cloud computing. Most of the frameworks overlooked the security of user's data privacy, data storage and energy preserving data sharing. To address all these security issues, the data security plan needs to be developed which reduces the security risks and also to cut costs and complexity to adopt the cloud computing environment. It is essential to keep in mind that the designing of the future framework solutions should be more cost effective and should provide better security and performance today.

REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5] Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] Y. Tang et al., "Secure Overlay Cloud Storagewith Access Control and Assured Deletion,"*IEEE Trans. Dependable and Secure Computing*,vol. 9, no. 6, 2012, pp. 903–916.

[7] R.L. Rivest, A. Shamir, and L. Adleman, "AMethod for Obtaining Digital Signatures andPublic-Key Cryptosystems," *Comm. ACM*, vol.21, no. 2, 1978, pp. 120–126.

[8] J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, "Provable datapossession of resource constrained mobile devices in cloud computing," Journal of Networks June 7, 2011.

[9] W.K. Wong et al., "Security of Outsourcing ofAssociation Rule Mining," *Proc. Int'l Conf. VeryLarge Databases* (VLDB 07), 2007, pp. 111–122.

[10] S. Yu et al., "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE Conf. Computer Comm. (INFOCOM 10), 2010, pp. 1–9; doi:10.1109/ INFCOM.2010.5462174.

[11] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. ACM Conf. Computer and Comm. Security, 2010, pp. 735–737.

