International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 2, April 2014)
National Conference on Computing and Communication-2014 (NCCC'14)

Security Challenges In Cloud Computing

S. Srinivasan[1], K. Raja[2]

[1]*Research Scholar, Research & Development Center, Bharathiar University,Coimbatore & Associate Professor, Department of M.C.A, K.C.G College of Technology, Chennai, Tamilnadu, India.*
[2]*Dean Academics, Alpha College of Engineering, Chennai, Tamilnadu, India.*

effectivemail@yahoo.com, raja_koth@yahoo.co.in

***Abstract*—Cloud computing is a standard futuristic computing model for the society to implement Information Technology and associated functions with low cost computing capabilities. Cloud computing provide multiple, unrestricted distributed site from elastic computing to on-demand conditioning with vibrant storage and computing requirement ability. Despite the probable gains attained from cloud computing, the security of open-ended and generously available resources is still hesitant which blows the cloud implementation. The security crisis becomes enlarged under the cloud model as an innovative measurement enter into the problem size related to the method, multitenancy, layer confidence and extendibility. This paper introduces an in-depth examination of cloud computing security problem. It appraises the problem of security from the cloud architecture perspective, cloud delivery model viewpoint, and cloud characteristics manner. The paper examines quite a few of the key research get together of performing cloud-aware security exposition which can reasonably secure the transforming and dynamic cloud model. Based on this investigation it presents a consequent comprehensive specification of cloud security crisis and main features that must be covered by proposed security solution for the cloud computing.**

***Keywords*-Cloud computing security; Cloud Security model;**

I. INTRODUCTION

Cloud computing is a resource delivery and usage model. It means to obtain resource where by shared software, hardware, and other information are provided to computers and other devices as a metered service via network[1]. Cloud computing is the next development of distributed computing paradigm which provides for extremely resilient, resource pooling, storage, and computing resources[2]. Cloud computing has motivated industry, academia, businesses to implement cloud computing to host heavy computationally exhaustive applications down to light weight applications and services.

The cloud providers should focus on privacy and security issues as an affair of high and urgent priority. The cloud providers have Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as Service (SaaS) and many services to present. A cloud service has distinct characteristics such as on-demand self service, ubiquitous network access, resource pooling, rapid elasticity and measured service. A cloud can be private or public cloud.

Cloud computing services afford fast access to their applications and diminish their infrastructure costs. As per Gartner survey, the cloud market was worth USD138 billion in 2013 and will reach USD 150 billion by 2015[3]. These revenues imply that cloud computing is a potential and talented platform. Even though potential payback and revenues could be realized from the cloud computing model, the model still has a set of open questions that force the cloud creditability and reputation.

Cloud security is a large set of policies, technologies, controls, and methods organized to protect data, applications, and the related infrastructure of cloud computing[3].

The major multiple issues [4] in cloud computing are:

- Multi-tenancy
- Cloud secure federation
- Secure information management
- Service level agreement
- Vendor lock-in
- Loss of control
- Confidentiality
- Data integrity and privacy
- Service availability
- Data intrusion
- Virtualization vulnerability
- Elasticity

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 2, April 2014)
National Conference on Computing and Communication-2014 (NCCC'14)

In this paper we analyze the few security issues involved in the cloud computing models. This paper is organized as follows. Section II discusses several security risks in cloud environment. In section III, analysis a short description of few related precise issues of cloud security. In section IV, describes integrated security based architecture for cloud computing. Section V shows current solutions for the issues of cloud environment. Finally, section VI concludes the paper and describes the future work for secure cloud computing.

II. Security Risks In Cloud Environment

Although cloud service providers can provide benefits to users, security risks play a vital role in cloud environment [5]. According to a current International Data Corporation (IDC) survey, the great argument for 74% of CIOs with respect to cloud computing is security[6]. Protecting the information such as sharing of resources used by users or credit card details from malicious insiders is of critical importance. A huge datacenter involves security disputes such as vulnerability, privacy and control issues related to information accessed from third party, integrity, data loss and confidentiality[7].

According to Tabaki et al. in SaaS, cloud providers are responsible for cloud security services and privacy of application services than the clients[8]. This task is relevant to the public than private cloud environment because the users require rigorous security requirements in public cloud. In PaaS, clients are responsible for application which runs on the different platform, while cloud providers are liable for protecting one's client's application from others. In IaaS, users are responsible for defending operating systems and applications, whereas cloud providers must afford protection for client's information and shared resources [9].

Ristenpart et al. insists that the levels of security issues in cloud environment are different. Encryption techniques and secure protocols are not adequate to secure the data transmission in the cloud[9]. Data intrusion of the cloud computing through the computer networks by illegal users require to be addressed and cloud computing environment needs to be secure and private for clients [10].

We will deal with few security factors that mainly affect clouds, such as data intrusion and data integrity. Cachin et al. represents that when multiple resources such as devices are synchronized by single user, it is hard to deal with the information corruption problem[11].

One solution is to utilize a byzantine fault tolerant replication protocol within the cloud environment. Hendricks et al. affirms that this solution can evade information corruption caused by several elements in the cloud[12]. In order to reduce risks in cloud environment, users can use encryption and decryption technique to defend the data and sharing of resources in cloud computing . Using hash function is a solution for data integrity by keeping short hash in local memory[13].

Garfinkel, states that, a different security risk that can happen with a cloud service provider is data intrusion. Amazon allows a missing password to be rearranged by short message service (SMS), the hacker may be able to log in to the electronic mail identification account, after receiving the new reorganized password[14].

Service hijacking allows attackers to concession the services such as sessions, email transactions there by launching malicious attacks such as phishing, and exploitation of vulnerabilities.

III. Issues Of Cloud Security

There are many security issues associated with number of dimensions in cloud environment.

Gartner states that, specific security issues: multi-tenancy, service availability, long-term viability, privileged user access and regulatory compliance[15].

Multi-tenancy shows sharing of resources, services, storage and applications with other users, residing on same physical or logical platform at cloud provider's premises. Defense-in-depth approach is the solution for multi-tenancy involves defending the cloud virtual infrastructure at different layers with different protection mechanisms[16].

An additional crisis in cloud services is service availability. Amazon mentioned authorization certificate is possible that can assure the service may be unavailable from time to time[17]. The users request service may terminate for any reason, which will break the cloud policy or no charge to cloud provider for this failure. Cloud providers found to protect services from failure need measures such as backups, Replication techniques and encryption methods such as HMAC technology are combined together to solve the service availability issue[18].

Another cloud security issue is long-term viability. Preferably, cloud service provider will never broke or obtain and swallowed up the information by large company.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 2, April 2014)
National Conference on Computing and Communication-2014 (NCCC'14)

But user must be ensuring their data will remain available even after any event may occur. To secure and protect the data in reliable manner through combining service level agreements or law enforcement and establishment of legacy data centers.

Privileged user access and regulatory compliance is major concern in cloud security[19]. According to Arjun kumar et al., Authentication and Audit control mechanism, Service level agreements, Cloud secure federation with single sign on, Session key management and Identity, Authentication, Authorization, and Auditing (IAAA) mechanisms, will protect information and restrict unauthorized user access in cloud computing[20,21].

IV. Integrated Security Based Cloud Computing Model

The integrated security based model for cloud environment is ensuring security in sharing of resources to avoid threats and vulnerabilities in cloud computing. To ensure security on distribution of resources, sharing of services, service availability by assimilate cryptographic methods, protective sharing algorithm and combine JAR files (Java ARchive) and RAID (redundant array of inexpensive or independent disk) technology with cloud computing hardware and software trusted computing platform. The integrated security based cloud computing model is shown in Figure 1.

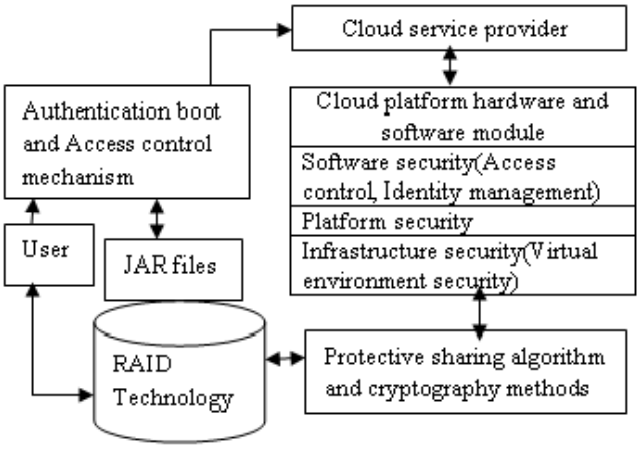

Figure 1. Integrated security based cloud computing model

The model uses a hierarchical protecting architecture with two layers. Each layer has its own tasks and incorporate with each other to ensure data security and to avoid cloud vulnerabilities in integrated security based cloud environment.

The authentication boot and access control mechanism layer, gives the proper digital signatures, password protective method, and one time password method to users and manages user access permission matrix mechanism. Authenticated boot service monitor software is booted on the computer and it keeps track of audit log of the boot process.

The integration of protective sharing algorithm and cryptography methods with redundant array of inexpensive disk layer advances the technologies in service availability. The model improves the efficiency of multi-tenancy and protects the information provided by the users. The protective cloud environment provides an integrated, wide-ranging security solution, and ensures data confidentiality, integrity and availability in integrated security based cloud architecture.

To construct the autonomous protection of secure cloud by association with security services like authentication and confidentiality. It reduces the risk of data intrusion, and verifies the integrity in cloud environment.

The cloud platform hardware and software module holds the software security, platform security, and infrastructure security. The software security provides identity management, access control mechanism, anti spam and virus. The platform security holds framework security and component security which helps to control and monitor the cloud environment. The infrastructure security make virtual environment security in integrated security based cloud architecture.

The cloud service provider controls and monitor the privileged user access and regulatory compliance by service level agreement through auditing mechanism.

We can use the protective sharing algorithm and cryptography methods to describe security and sharing of resources and services on cloud computing:

$$B_s = A(\text{user-node});$$

$$D_s = F * B_s + K_i$$

A(.) : Access to user nodes, an application server of the system is denoted by user-node in the formula;

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 2, April 2014)
National Conference on Computing and Communication-2014 (NCCC'14)

B_s : Byte matrix of the file F;

D_s : Byte of data files in global center of system;

K_i : User key

F : File, file F in user-node are represented as follows: F={F(1), F(2), F(3), ….F(n)}, file F is a group of n bytes of a file.

Based on the values of information security of cloud environment, design protective sharing algorithm with cryptography methods such as encryption which maintains a protective secret key for each machine in integrated security based cloud computing model indicated as follows:

B_s=A(user-node);
B_s=P.B_s + K_i
D_s=E(F).B_s
of which:
A_s(.) : Authorized application server;
B_s : Byte matrix in protected mode;
P : Users' protective matrix;
E(F) : Encrypt the byte of file F;

The above integrated security based protective sharing algorithm in cloud environment can be represented mathematically in form of deterministic finite automata.

A deterministic finite automata is represented formally by a 5-tuple (Q,Σ,δ,q_0,F), where: Q is a finite set of states, Σ is a finite set of symbols, δ is the transition function, that is, $\delta: Q \times \Sigma \rightarrow Q$. q_0 is the start state, that is, the state of the automaton before any input has been processed, where $q_0 \in Q$. F is a set of states of Q (i.e. $F \subseteq Q$) called accept states.

The following Deterministic Finite Automata (DFD) state diagram represents the integrated security based protective sharing algorithm as shown in Figure 2.

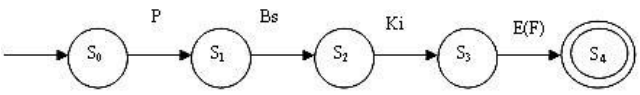

Figure 2. DFD-State diagram for integrated security based protective sharing algorithm

where S_o : start state
S_1,S_3 : intermediate states
S_4 :final state or accept state
P, Bs, K_i, E(F) : input symbols.
of which initially B_s=A(user-node);

In automata theory, a state transition table is a table showing what state finite state machine will move to, based on the current state and other inputs. A state table is essentially a truth table in which some of the inputs are the current state, and the outputs include the next state, along with other outputs.

The following Deterministic Finite Automata (DFD) state transition table for the above DFD-State diagram as shown in Table 1.

Table 1.
state transition table

input states	input symbols			
	P	Bs	K_i	E(F)
S_o	S_1	-	-	-
S_1	-	S_2	-	-
S_2	-	-	S_3	-
S_3	-	-	-	S_4

The integrated security based cloud computing model adopts a multi-dimension architecture of two layer defense in cloud environment. The RAID (redundant array of independent disk) assures data integrity by data placement in terms of node striping. The cloud service provider audits events, log and monitoring happenings in the cloud environment.

V. Current Solutions For The Issues In Cloud Environment

In order to reduce threats, vulnerability, risk in cloud environment, consumers can use cryptographic methods to protect the data, information and sharing of resources in the cloud computing [22]. Using a hash function is a solution for data integrity by maintaining a small hash memory.

Bessani et al. use Byzantine fault-tolerant method to provide and store data on different clouds, so if one of the cloud providers is out of order, they are still able to store and retrieve information accurately[18].

Bessani et al, use a Depsky system deal with the availability and confidentiality in cloud computing architecture. Using cryptographic methods, one can store the keys in cloud environment through secret sharing algorithm to hide the values of the key from attackers.

Encryption is measured solution by Bessani et al. to address the issue of loss of data.

Munts-Mulero discussed the issues of existing privacy protection technologies like K anonymous faced when applied to large information and analyzed the current solutions [23].

Sharing of account credentials between customers should be strictly denied by deploying strong authentication, authorization and auditing mechanism by cloud service provider for consumer session[24]. The consumer will be able to allow HIPS (Host Intrusion Prevention System) at customer end points, in order to achieve confidentiality and secure information management.

The integrated based security model provides a RAID technology with sharing algorithm and cryptographic method. It assures data integrity and service availability in cloud computing architecture. The authentication boot and access control mechanism ensure security through cloud deployment models.

VI. Conclusion And Future Work

It is clear that, although the use of cloud computing has rapidly increased. Cloud security is still measured and the important concern in the cloud computing environment. To achieve a secure paradigm, this paper focused on vital issues and at a minimum, from cloud computing deployment models view point, the cloud security mechanisms should have the enormous flair to be self defending with ability to offer monitoring and controlling the user authentication, access control through booting mechanism in cloud computing integrated security model. This paper proposes a strong security based cloud computing framework for cloud computing environment with many security features such as protective sharing of resources with cryptography methods along with the combination of redundant array of independent disk storage technology and java archive files between the users and cloud service provider. The analysis show that our proposed model is more secure under integrated security based cloud computing environment and efficient in cloud computing.

Future research on this work may include the development of interfaces, standard and specific protocols that can support confidentiality and integrity in cloud computing environment. We will make the actual design more practical and operational in the future. To welcome the coming cloud computing era, solving the cloud security issues becomes extreme urgency, that lead the cloud computing has a bright future.

REFERENCES

[1] Guoman Lin, "Research on Electronic Data Security Strategy Based on Cloud Computing", 2012 IEEE second International conference on Consumer Electronics,ISBN: 978-1-4577-1415-3, 2012, pp.1228-1231.

[2] Akhil Behl, Kanika Behl, "An Analysis of Cloud Computing Security Issues", 2012 IEEE proceedings World Congress on Information and Communication Technologies, ISBN: 978-1-4673-4805-8,2012,pp.109-114.

[3] Deyan Chen, Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing",2012 IEEE proceedings of International Conference on Computer Science and Electronics Engineering, ISBN: 978-0-7695-4647-6,2012,pp.647-651.

[4] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", IEEE Transactions on cloud computing,9(4), 2012, pp.5490-5499.

[5] J.Viega, "Cloud computing and the common man",Computer,42,2009,pp.106-108.

[6] Clavister,"Security in the cloud", Clavister White Paper, 2008.

[7] C.Wang,Q.Wang,K.Ren and W.Lou,"Ensuring data storage security in cloud computing",ARTCOM'10:Proc. Intl.Conf. on Advances in Recent inTechnologies in Communication and Computing,2010,pp.1-9.

[8] H.Takabi,J.B.D.Joshi and G.J Ahn,"Security and Privacy Challenges in Cloud Computing Environments",IEEE Security & Privacy,8(6),2010,pp.24-31.

[9] T.Ristenpart,E.Tromer ,H.Shacham and S.Savage, "Hey you,get off of my cloud:exploring information leakage in third-party compute clouds",CCS'09:Proc.16th ACM Conf. on Computer and communications security,2009,pp.199-212.

[10] S.Subashini and V.Kavitha,"A survey on security issues in service delivery models of cloud computing",Journal of Network and Computer Applications,34(1),2011,pp.1-11.

[11] C.Cahin,I.Keidar and A.Shraer,"Trusting the cloud",ACM SIGACT News,40,2009.pp.81-86.

[12] J.Hendricks, G.R.Ganger and M.K.Reiter,"Low overhead byzantine fault –tolerant storage",SOSP'07:Proc.21st ACM SIGOPS symposium on Operating systems principles,2007,pp.73-86.

[13] R.C.Merkle,"Protocols for public key crptosystems",IEEE Symposium on Security and Privacy,1980,pp.122-134.

[14] S.L.Garfinkel,"Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy,1(6),2003,pp.20-26.

[15] Gartner:Seven cloud computing security risks.InfoWorld,2008-07-02, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[16] Microsoft Research, Securing Microsoft's Cloud Infrastructure", in White Paper, 2009.

[17] Amazon,Amazon Web Services, Web Services licensing agreement, October 3,2006.

[18] A.Bessani,M.Correia, B.Quaresma, F.Andre and P.Sousa,"DkpSky:dependable and secure storage in a cloud-of-clouds",EuroSys'11:Proc.6th Conf. on Computer systems,2011,pp.31-46.

[19] Arjunkumar, Byung gook Lee, Hoon Jae Lee,Anukumari,"Secure Storage and Access of Data in Cloud Computing", 2012 IEEE ICT Convergence,ISBN:978-1-4673-4828-7,2012,pp.336-339.

[20] M.S.Blumental,"Hide and Seek in the Cloud", IEEE Security and Privacy, IEEE,11(2),2010,pp.57-58.

[21] Akhil Behl, KanikaBehl,"Security Paradigms for Cloud Computing", 2012 IEEE Fourth International Conference on Computational Intelligence, Communication Systems and Networks,ISBN:978-0-7695-4821-0,2012,pp.200-205.

[22] R.C Merkle,"Protocols for public key cryptosystems",IEEE Symposium on Security and Privacy,1980.

[23] Muntes-Mulero V, Nin J. Privacy and anonymization for very large datasets In:Chen P,ed. Proc of the ACM 18th Int'l Conf. on Information and Knowledge Management, CKIM 2009, New York:Association forComputingMachinery,2009,2117.2118,[doi:10.1145/1645953.1646333].

[24] Wikipedia-Cloud Computing security.