ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey on Data Security and Privacy Protection Issues in Cloud Computing

Amit Kumar Pillai [1], Prof. Anshul Khurana[2]

Research Scholar, Department of Computer Science Engineering, Shri Ram Institute of Technology - [SRIT], Madhya Pradesh, India[1]

Professor & Guide, Department of Computer Science Engineering, Shri Ram Institute of Technology - [SRIT], Madhya Pradesh, India[2]

ABSTRACT: Cloud computing has recently emerged as a new paradigm for hosting and delivering services over the Internet. Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand. However, despite the fact that cloud computing offers huge opportunities to the IT industry, the development of cloud computing technology is currently at its infancy, with many issues still to be addressed. In this paper, we present a survey of cloud computing, highlighting its key concepts, architectural principles, state-of-the-art implementation as well as research challenges. The aim of this paper is to provide a better understanding of the design challenges of cloud computing and identify important research directions in this increasingly important area.

KEYWORDS: cloud computing ; cloud computing security ; Third party audit ; Security objectives ; Data security concerns.

I. INTRODUCTION

In cloud infrastructure, organizations sensitive information is kept at geographically dispersed cloud platforms and this critical information is not under direct control of organization. So the security is important concern in cloud. Nowadays Use of Cloud computing is increasing day by day.Security in cloud cannot be simulated even though as different simulation tools available are like Cloud Reports, cloud Analyst,MR-Cloud Sim,Cloudsim.Securing data on cloud is one of the most challenging tasks. The cloud gives a platform for many types of services. In cloud storage systems, the data of a client is stored at a server which is at a remote location. The server which stores data of a client is not necessarily trusted. Hence it is necessary to check whether data stored on cloud is tampered or not. Also outsourcing of whole file system is difficult task. The client should not download all stored data to check the integrity of the data because it will lead to bandwidth and time problems. Cloud provider also cant be available always online to check the integrity of the data however data owner cant trust the cloud owner to handle the data as cloud owner himself can change the original data and there will be loss of integrity. If the hacker somehow gets access and takes data and changes it then this change is not even identified by service provider.So there will be necessity of third party audit which will ensure integrity of the data. Third party is used as gateway between client and cloud which is used for crypto-box or develop program helpful for encryption-decryption mechanism [3].Cloud storage should be such that users can use it as if it is a local. Users shouldnt bother about integrity of data. Thus following schemes [4] given digital signature algorithm to give privacy and integrity of data in cloud computing.Mainly there are 6 attack surfaces in cloud such as service instance towards a user, cloud system, service instance against the cloud system, cloud system toward the user, user towards the cloud provider etc.[5].These 6 attack surfaces are shown in figure 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

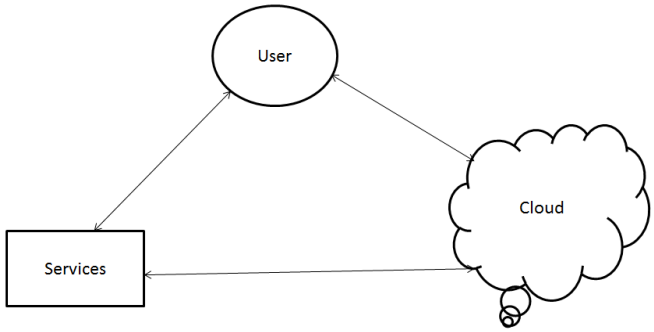

Fig. 1: Cloud Computing triangle & its 6 attack surfaces

Service instance towards a user consist of buffer overflow attack.Sql injection or privilege escalation. In [6] proposed a protocol in which there are 3 participants: Cloud service provider (CSP), Third party auditor (TPA) and CO (Cloud owner). They have ensured correctness of data in the cloud by mechanism which provides data integrity, confidentiality and privacy. The algorithms they have used are RSA algorithm, Hash function along with several cryptography tools to pro- vide security to data stored on cloud. Cloud requires lower investment where customer does not required to purchase the resources, thats why its the favorite of startup companies as they do not need heavy investment in setting up of IT firm.

Cloud has many challenges like Versatility, scalability, interoperability, security, diagnosis and automation [7].In most of the cases security is considered as extra parameter to extend software and not as essential part of development process .So the security should be considered as important

part of development process in software development life cycle. Normally software development life cycle consist of communication, planning, modeling construction, deployment, maintenance and testing as activities [8].In cloud security, data security is important factor. Monitoring Data is to be transferred from monitored entity to analytics engine. This various data that go across public cloud datacenters , internet backbone switches, Telco networks, transoceanic optical fibers and so on should be secured.The person at a distance can attest the current configuration of a platform . So modifications made by unauthorized administrators or privileged malicious users can be recorded[9] .Through the use of TPA we are eliminating the need of client to check the integrity of the data. But there is need of data dynamics to be considered because data can be changed due to multiple reasons such as block modification, insertion and deletion. So there is need of data dynamics and public audit ability[10]. Rewagad [11], have given algorithm of using digital signature and Diffie Hellman key exchange with (AES). Advanced Encryption Standard is used for confidentiality of data. encryption algorithm to protect confidentiality of data stored in cloud. Due to this though the key in transmission is hacked, DH-key exchange makes it of no use because key in transit is of no use if there is no users private key. This architecture makes it difficult for hacker to crack the system so there is protection to data.

II. CLOUD INFORMATION SECURITY OBJECTIVES

Cloud computing gives many advantages like scalability,

A. Confidentialty

Confidentiality can be defined as there should not be dis- closure of data to unauthorized persons. It is only authorized users having access to protected data and having permission to access data. It ensures user data which resides in cloud and cant be accessed by unauthorized party[17]. Confidentiality in cloud system corresponds to various areas as shown in table .1

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

TABLE I: Areas in Confidentiality Table

Confidentiality have relation with areas	Area consist of /Accomplished By	Description
Intellectual property rights	Inventions designs artistic ,musical and literacy work	Intellectual Property (IP) should be protected legally.
Covert channel	Timing of messages or inappropriate use of storage mechanism	Attack responsible to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.
Traffic analysis	concentrate on rate and volume of traffic.	for restricting this there should be constant rate of message traffic.
Encryption	converting messages from readable format to unreadable format	Process of Encoding messages.
Inference	Database security	Ability to use and relate information protected at higher security leage.

Description

Intellectual Property (IP) should be pro- tected legally.
Attack responsible to transfer information objects between pro- cesses that are not supposed to be al- lowed to communi- cate by the computer security policy. for restricting this there should be con- stant rate of message traffic.self-provisioning and elasticity but there are some security risks and its inability to guarantee confidentiality and privacy of consumer data [12].Service providers security is important because data has to be protected before getting stored in the cloud which can cause data unsafe in server side [13].There Encryption converting messages from readable format to unreadable format Process of Encoding messages.are various paths when communication takes place between any 2 mobile devices. Vulnerabilities which are available in different paths need to be identified and how cloud computing can be used to give security to files, messages, m-commerce transactions etc.[14] . Software should have following 3 prop- erties to be considered secure.

1) Dependability: Software which is able to work error-free though attack take place or running under a malicious host.
2) Trustworthiness: There should be minimum number of vulnerabilities or no vulnerabilities in software. It must be able to resistant to malicious logic
3) Survivability (Resilience): Cloud should be able to resist attacks and the attacks which are not possible to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

resist should be able to tolerate. Those attacks which cant be tolerated and if any damage occurs during the attack cloud should be able to recover from that type of attack [15].

Software assurance is necessary in cloud computing.[16]. Also other 7 principles which are needed in security which are described as follows.Inference Database security Ability to use and re- late information pro- tected at higher secu- rity leage.

B. Integrity

For integrity following 3 principles should meet.

1) There should not be any modification to data by unau- thorized person or process.
2) Unauthorized alteration of data should be done by au- thorized person or authorized persons.
3) The internal information is consistent; external situation.

C. Availability

It guarantees reliable and anytime access to cloud data or cloud computing resources .To decide which cloud model should be used, Availability plays important role. Agreement emphasizes the trepidation of availability between data owner and cloud service provider [18].

Threat:

Dos attack
Reverse of CIA (Confidentiality, integrity, availability) triad is DAD (disclosure, alteration, destruction.)

D. Authentication

It is related to users identity. Eg. User presents userID to computer login page and then has to give password. The authentication is done by system of cloud user.This authenti- cation is done by verification of password.

E. Authorization

It can be defined as rights to be given to particular indi- vidual.Though the person is authenticated one cant access the resources and information asset of another person.It all comes under authorization .When user is authenticated,privileges to user are determined. Authorization process is based on attributes can be in the form of digital certificates[19].

F. Auditing

To maintain operational assurance, organization uses 2 basic methods such as System audits and monitoring .Cloud customer or cloud provider both can use auditing. IT auditors are divided into 2 types:

Internal auditors: Internal auditors work for specific organi- zation. They have more scope than external auditors such as checking for compliance and standards of due care, auditing operations of cost efficiencies and recommending appropriate controls.

IT auditors audit functions such as contingency plans, data center security, Data library procedures, backup controls, system development standards, system transaction controls.

G. Accountability

It can be defined as ability to determine actions and be- haviors of a person within a cloud and to identify that par- ticular person. Accountability corresponds to non-repudiation. Audit trail and logs provide accountability .For performing postmortem studies to analyze historical events and persons or processes related to these events Accountability is used. To simplify accountability and audit ability[20] have described 3 layers such as data layer, workflow layer and system layer (network logs, operaing system and network logs) In the cloud, service provider have full access to client data and applications, which leads to illegitimate tampering or usage of client

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

data may not be detected. From clients side using federated cloud can cause increased risk, control over who can access and modify the client data .

III. DATA SECURITY CONCERNS

Security mainly depend on 3 parameters i.e. confidentiality, integrity and availability which causes a major issue for cloud owner and data users. [21]. Threats to infrastructure data and access control: Threat can be defined as an event, which can cause damage to system and create loss of CIA triad .Vulnerability can be defined as weakness in system that can be exploit by threat. Many of the threats occur due to trust relationship issues Between cloud service provider and cloud user. Eg. Cloud service provider doesnt trust their clients and can think that they can take advantage of available policies and privacy laws and run malware attacks. Whereas cloud customers may think that cloud service provider may try to hide their company policies [22]. Common threats to cloud security:

1) Eavesdropping: Shoulder surfing, data scavenging, traf- fic analysis ,Finding pretext of information,social engi- neering, dumpster diving ,sniffing, keystroke monitoring are all types of eavesdropping to gather or reconnais- sance the information.
2) Fraud: Collusion, data manipulation, falsified transac- tion, and other change of data integrity i.e. modification of information are the examples of fraud.
3) Theft: Physical theft of hardware or software, to stole the secret information for benefight is example.
4) Sabotage: DOS attacks data integrity sabotage, produc- tion delays are examples.
5) External attack: Malicious cracking, scanning and prob- ing to gather infrastructure information, insertion of malicious code or virus are examples.

A. Reconnaissance Techniques

Reconnaissance is a term related to hacking. It means gathering as much information about target as possible before launching the attack. Reconnaissance can also be defined as range of information collecting activities that try to launch malicious packets. Reconnaissance techniques can be classi- fied as:

1) Low tech methods
2) General web searches (Internet Reconnaissance)
3) Who is databases? (IP and network reconnaissance)
4) DNS

These various methods and its defense are shown as follows: Social Engineering: Finding pretext to obtain privileged infor- mation or text Manipulate an individual conscience or sense of social norms
E.g. Helpdesk call asking for password
Defense: Instruct employees not to divulge sensitive informa- tion on phone, User awareness.
Physical Break-in: Walking past unlocked doors to data Defense: Insist on using badges for access, everyone must have badge lock sensitive equipment.
Dumpster Diving: Retrieving sensitive information from trash. Defense: Shared important documents
Internet Reconnaissance Tools used Internet search engines Usenet tools: Data derived from company website from inter- net, Data obtained employee information, Business Partners etc.
Defense: Not to post any sensitive information. Instruct em- ployees what to post and what not .Find what posted about you and company.
DNS reconnaissances-Zone transfer: Used to harvest data. Information obtained from DNS.Information obtained from DNS can be Range of addresses used, Address of mail server,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Address of web server, Operating system information and Comments. In zone transfer, content of DNS zone file are as it is copied from primary DNS server to a secondary DNS server.
Defense: Provide only necessary information. No operating system and comment information .
Restrict zone transfer: Allow only for necessary hosts.

B. Denial of service

Denial of a service consists of variety of techniques de- signed to deny users or client access to specific system and network resources. In denial of service attacks following types of resources are targeted:

1) CPU utilization
2) Network bandwidth
3) Memory utilization
4) Disk space and input-output.

Most common example of denial of service attack is the distributed DoS (DDoS). This is based on traffic volume as the target is flooded with illegitimate requests thus prevents targets ability to process legitimate traffic[23]. Following are the Techniques for denial of service.

1) Buffer overflows
2) Malformed packet data
3) Packet flooding

C. Account Cracking

Account cracking also known as password cracking. It refers to cracking single password hash or encrypted i.e. hashed password file by using various account cracking tools. In this hashed password are captured using sniffers from network. Brutus, Web cracker, Obiwan, burp intruder, burp repeater these are the web password cracking tools.

Following are the techniques for account or password crack-
ing:

1) Dictionary password attack: A set of words is run against user account.
2) Brute force password attack: Every combination of char- acter is tried until the password is cracked.
3) Hybrid attack: It is combination of brute force password attack and dictionary password attack.

D. Hostile and self replicating codes

It consists of viruses, worms, backdoors, logic bombs, spyware.
Viruses-Viruses are the hostile programs that depend on user for replicating
Worms-These are self replicating
Backdoors-Through installation of foreign code on system allow un-authorized access.
Logic bombs-These are attached by attacker to attack on system to legitimate commercial software. These are triggered by specific date or specific combination of system events. Spyware-These are covert applications installed in a system for gathering predefined information.
Trojan horses-Unlike worm Trojan horse does not typically self replicate. It can be defined as unauthorized program contained within a legitimate program. Trojan horses can enter to computer through freeware, physical installation,e- mail attachments, or infected websites

E. System or network penetration

Following are the techniques for System or network pene- tration

1) Session-Hijacking
2) Sniffing
3) Cache exploits
4) State-Based attacks
5) Firewall attacks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

6) IDS attacks
7) Session ID hacking

F. Buffer overflow

This attack happens when program allocates certain fixed memory block for something but then attempt to store more data than allocated space. Due to overflowing of data there can be problem in normal execution of data. These can be detected by boundary testing and manual auditing of code.

G. Sql injection Attack

It occurs when SQL query strings are concatenated with variables. Target of SQL injection attack is data in database.For preventing SQL injection attack prepared queries are used.

H. Malware injection attack

In cloud environment, attacker can take advantage of ex- change of metadata information .Metadata exchange occurs between web server and web browser as in cloud systems the clients request is based on authentication and authorization. Saltzer and Schroeder of university of Virginia has given protection of information stored in computer system by fo- cusing on hardware and software issues that are required to provide information protection [25]. Attacker may intrude with malicious code or inject malicious service. If attack gets successful then cloud service will suffer from eavesdropping and deadlocks .which leads to authorized users to wait for long time .

I. Cross Site scripting Attack (XSS)

Cross site scripting attack occurs when user input is directly passed to templates.Hacker or Attacker can inject HTML/JavaScript into the page to take the users session, log keyboard entries,also attacker can do DDOS attacks on other websites or other malicious actions.Though some softwares uses content security policy to resist execution of inline javascript code developers are still required to prevent cross site scripting attack.CSP is just another layer of defense that is not implemented in all webbrowsers.

IV. CONCLUSION

Firstly computer software was not written considering se- curity as important factor but due to increasing frequency of attacks against cloud system newly softwares include security as a prime concern. Thus cloud computing is wide area so it encompasses so many threats due to its vulnerabilities . We have to compromise with one either security or performance. So Technicians should find a way to build a system which is secure enough for everyday use while possessing reasonable performance and reliable characteristics. It is big challenge to solve security issues in cloud.

REFERENCES

[1] D. Dev and K. Baishnab, "A review and research towards mobile cloud computing," in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on*, April 2014, pp. 252–256.
[2] "Cloud security alliance guidance version (http://www.cloud-security alliance.org/guidance/csaguide.pdf)," September 13 2.1,2009.
[3] A. Jaber and M. Bin Zolkipli, "Use of cryptography in cloud computing," in *Control System, Computing and Engineering (ICCSCE), 2013 IEEE International Conference on*, Nov 2013, pp. 179–184.
[4] H. K.Govinda, V.Gurunathprasad, "Third party auditing for secure data storage in cloud through digital signature using rsa," in *International journal of advanced scientific and technical researc*, August 2012.
[5] D. M. S. Ajey Singh, "overview of attacks on cloud computing," in *International journal of engineering and innovative technology(IJEIT)*, April 2012.
[6] P. Garg and V. Sharma, "An efficient and secure data storage in mobile cloud computing through rsa and hash function," in *Issues and*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Chal- lenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, Feb 2014, pp. 334–339.

[7] J. Martin-Flatin, "Challenges in cloud management," *Cloud Computing, IEEE*, vol. 1, no. 1, pp. 66–70, May 2014.

[8] W. Goertzel K. and T. al, "Enhancing the development life cycle to produce secure software," *Draft version 2.0 Rome,New york:United states department of defense data and analysis center for software*, 2008.

[9] D. Wallom, M. Turilli, G. Taylor, N. Hargreaves, A. Martin, A. Raun, and A. McMoran, "mytrustedcloud: Trusted cloud infrastructure for security-critical computation and data managment," in *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*, Nov 2011, pp. 247–254.

[10] W. L. Qian Wang Cong Wang Kui Ren and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, May 2011.

[11] P. Rewagad and Y. Pawar, "Use of digital signature with diffie hellman key exchange and aes encryption algorithm to enhance data security in cloud computing," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, April 2013, pp. 437–439.

[12] M. Jog and M. Madiajagan, "Cloud computing: Exploring security design approaches in infrastructure as a service," in *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 Inter- national Conference on*, Dec 2012, pp. 156–159.

[13] V. Nirmala, R. Sivanandhan, and R. Lakshmi, "Data confidentiality and integrity verification using user authenticator scheme in cloud," in *Green High Performance Computing (ICGHPC), 2013 IEEE International Conference on*, March 2013, pp. 1–5.

[14] V. Anne, J. Rao, and R. Kurra, "Enforcing the security within mobile devices using clouds and its infrastructure," in *Software Engineering (CONSEG), 2012 CSI Sixth International Conference on*, Sept 2012, pp. 1–4.

[15] "Information assurance technology analysis center(iatac),data and anal- ysis center for software (dacs),software security assurance ,state-of-the art report(soar)," July 31 2007.

[16] a. B. K. D. Komaroff, M., "software assurance initia- tive(https://acc.dau.mil/communitybrowser.aspx?id=25749)," September 13 2005.

[17] H. Tianfield, "Security issues in cloud computing," in *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*, Oct 2012, pp. 1082–1089.

[18] S. Ramgovind, M. Eloff, and E. Smith, "The management of security in cloud computing," in *Information Security for South Africa (ISSA), 2010*, Aug 2010, pp. 1–7.

[19] A. Albeshri and W. Caelli, "Mutual protection in a cloud computing environment," in *High Performance Computing and Communications (HPCC), 2010 12th IEEE International Conference on*, Sept 2010, pp. 641–646.

[20] W. J. Mpofu, Nkosinathi; van Staden, "A survey of trust issues con- straining the growth of identity management-as-a-service(idmaas)," in *Information Security for South Africa (ISSA), 2014*, August 2014, pp. 1–6.

[21] D. P. S. Jain, P.; Rane, "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment," in *Information and Communication Technologies (WICT), 2011 World Congress on*, Dec. 2011, pp. 456,461,.

[22] A. W. S. Khorshed, M.T.; Ali, "Trust issues that create threats for cyber attacks in cloud computing,," in *Parallel and Distributed Systems (ICPADS), 2011 IEEE 17th International Conference on*, Dec. 2011, pp. 900,905,.

[23] B. van Niekerk and P. Jacobs, "Cloud-based security mechanisms for critical information infrastructure protection," in *Adaptive Science and Technology (ICAST), 2013 International Conference on*, Nov 2013, pp. 1–4.

[24] M. Djenna, A.; Batouche, "Security problems in cloud infrastructure," in *Networks, Computers and Communications, The 2014 International Symposium on*, June 2014, pp. 17–19.

[25] J. Saltzer and M. Schroeder, "The protection of information in computer systems," in *Fourth ACM symposium on operating systems principles*, October 1974.