IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Cloud Security Issues, Techniques and Concerns – An Overview

V. Negi[1*]

[1] Computers, School of Technology Management & Engineering, NMIMS, Navi Mumbai, India

[*]*Corresponding Author: variza9@gmail.com, Tel.: +91-79777-84745*

Available online at: www.ijcseonline.org

Accepted: 20/Jan/2019, Published: 31/Jan/2019

***Abstract*—** Among cloud computing resources like networks, servers, storage, applications and services, Storage is one of the major resource that is being used at large by the cloud users. Small to mid-sized business houses use Storage-as-a-Service to enhance business availability and reliability, managing backups and to extenuate risks involved in disaster recovery. Security, therefore, becomes the most critical aspect due to the confidential and intimate information being stored on the public cloud. In public cloud, since the services are being provided by the third party service providers, which are geographically dispersed and involve resources outside the user's premises, the three service models (IaaS, PaaS, SaaS) face serious security threats. Public cloud can fall prey to threats like Data breaches, insufficient identity, insecure APIs, system vulnerabilities, account hijacking, malicious insiders, data loss, insufficient due diligence, DoS and abuse of cloud services. This paper presents a review on the most pressing security issues within cloud computing, the techniques that can be employed in addressing such cloud security issues and the challenges.

***Keywords*—** Cloud Computing, Security Issues, Cloud Security, Cloud Data Storage Security

I. INTRODUCTION

With the ability to dynamically provision the resources like processors, network, memory and storage, more organizations are adopting Cloud Computing. Even the hand held devices like Smartphones, PDAs and Laptops are using the services of Cloud these days [9] [10]. Cloud Security Alliance (CSA) predicts that over 70 percent of the world's businesses today operate on the cloud. A cloud has so much to offer like on-demand self-service, broad network access, pooling of computing resources rapidly, elastically and lower fixed costs. Thus 70 percent in the market share is fair enough.

Rest of the paper is organized as follows, Section I contains the introduction of Cloud Computing, Section II contain the related work of Cloud growth, Section III contain the security issues in Cloud, Section IV contain a review of cloud security models based on their underlying techniques, Contributions and drawbacks, section V concludes research work with future directions.

II. CLOUD GROWTH

From 2015 through 2020, the rate of IT spending in case of Cloud computing has been predicted to grow more than 6 times. The most employable model of Cloud computing which is Public Cloud, will have increased worldwide spending from $67B in 2015 to $162B in 2020, according to International Data Corporation (IDC) [11].

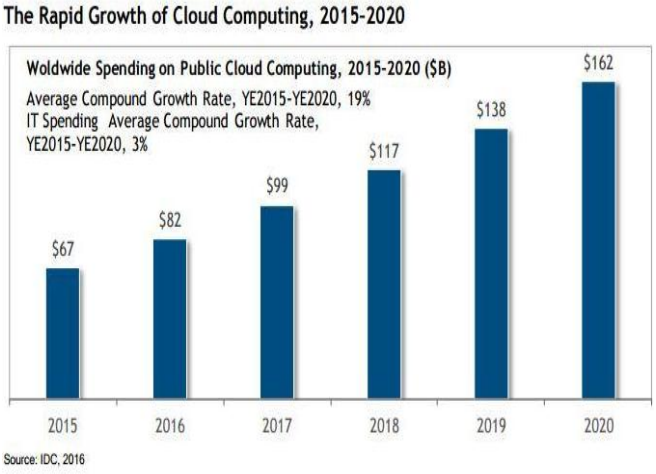

Figure 1. Worldwide spending on Cloud Computing [11]

Gartner predicts the worldwide public cloud services market will grow to $383.3B in 2020, up from $209.2B in 2016. [12]

	2016	2017	2018	2019	2020
Cloud Business Process Services (BPaaS)	40,812	43,772	47,556	51,652	56,176
Cloud Application Infrastructure Services (PaaS)	7,169	8,851	10,616	12,580	14,798
Cloud Application Services (SaaS)	38,567	46,331	55,143	64,870	75,734
Cloud Management and Security Services	7,150	8,768	10,427	12,159	14,004
Cloud System Infrastructure Services (IaaS)	25,290	34,603	45,559	57,897	71,552
Cloud Advertising	90,257	104,516	118,520	133,566	151,091
Total Market	**209,244**	**246,841**	**287,820**	**332,723**	**383,355**

Source: Gartner (February 2017)

Figure 2. Worldwide public cloud services forecast (millions of Dollars) [12]

III. SECURITY ISSUES IN CLOUD

Cloud has its share of security threats and challenges. With so much data going into the cloud, public cloud particularly, cloud become natural targets for bad actors. CSA has conducted a survey of industry experts to compile professional opinions on the greatest security issues within cloud computing and released Industry Insights report on Security in Cloud [13] [14] [15]. Here are the top cloud security issues:

A. Data Breaches

One of the major potential threat to cloud data is inappropriate access by the cloud provider's staff to the sensitive and confidential data of the client, such as, financial information, individual intimate information, personal health information, trade secrets and intellectual property. According to application vulnerabilities, human errors and poor security practices can be major reasons for a data breach to occur. Safe policies and procedures should be in place to assure the cloud client of his data safety.

B. Insufficient Identity, Credential and Access Management

CSA has stated "Malicious actors masquerading as legitimate users, operators or developers can read, modify and delete data; issue control plan and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source. As a result, insufficient identity, credential or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users."

C. Insecure interfaces and application programming interfaces (APIs)

For interaction of Cloud users with the Cloud services, the cloud service providers release user interfaces or APIs. Resource provisioning, authentication, access control and monitoring, all are performed with these interfaces. So these APIs and interfaces must be robust enough as they take care about the security and availability of general cloud services. Thus they help in maintaining the confidentiality, integrity, and availability of the cloud.

D. System vulnerabilities

With the emergence of multi owner or multitenancy in cloud computing where enterprises share database, memory and other resources may give rise to new security concerns. Credulous bugs in programs (or in the operating system itself) which attackers can use to corrupt a system to steal data, taking control of the system or even disrupting service operations are basically system vulnerabilities.

E. Account hijacking

Account or service hijacking is a type of identity theft in which the hacker uses the stolen account information to carry out malicious or unauthorized activity. On acquiring the access to the user's credentials, they can eavesdrop on activities and transactions, return falsified information, manipulate data and even redirect users to illegitimate sites. This leads to compromising the confidentiality, integrity and availability of the system.

F. Malicious insiders

Insider threats include fraud, sabotage and theft or loss of confidential information caused by trusted insiders. They represent purposeful action on the part of insiders to act in opposition to the interests of the organization, whether for financial gain, retribution or some other motivation. Systems that depend solely on cloud service providers for security are at greater risk.

G. Advanced persistent threats (APTs)

In case of advanced persistent threats (APTs), an attacker does email-spoofing attack, a type of social engineering, to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a back door that bypasses the system's customary security mechanisms. The attacker further gathers valid user credentials and move laterally across the network, installing more back doors. APT attacks are thus difficult to identify, as they often adapt to the security measures intended to defend against them.

H. Data Loss

Data loss in cloud can occur due to many various reasons, other than just the malicious insiders. Data loss can occur due to accidental deletion by the cloud service provider or a physical catastrophe such as a fire or earthquake. Thus a cloud service provider ensures a cloud customer that he is taking adequate measures to back up data and also following the best techniques for business continuity and disaster recovery.

I. Insufficient due diligence

Organizations, when are designing their business strategies for growth, must suss out the type of cloud techniques and service providers being considered. Organizations must avoid plunging into adopting any random service providers and not having done their initial background checking, as this may expose themselves to the high security risks.

J. Abuse and nefarious use of cloud services

This security risk arises due to relatively poorly secured registration systems, free cloud service trials and fraudulent account sign-ups via payment instrument present in the cloud computing environment. This facilitates anonymity, due to which spammer, malicious code authors and criminals can attack the system. Distributed denial-of-service attacks, email spam and phishing sites are some of the examples of abuse and nefarious use of cloud services.

K. Denial of service (DoS)

DoS attack pose a major threat to the availability of services of the cloud to its users. The attacker can greatly degrade the quality or fully degrade the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space, or network bandwidth. Also in cloud environment, DoS can reduce the performance of cloud services significantly by damaging the virtual servers.

L. Shared technology vulnerabilities

Often in a multi-tenant architecture or multi-customer applications, the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation. Due to this, the delivery models are susceptible to shared technology vulnerabilities.

M. Bonus cloud threat for 2018: Spectre and Meltdown

Spectre and Meltdown is a hardware vulnerability affecting most modern microprocessors. It allows a rogue process to read all memory, even when it is not authorized to do so. Both of them permit side-channel attacks as they break down the isolation between applications. An attacker that is able to access a system through unprivileged log in, can read information from the kernel or attackers, can read the host kernel, if they are a root user on a guest virtual machine (VM). This is a major problem for the cloud service providers. There are patches available for making an attacker harder to execute an attack. As in certain cases, the patches might also degrade performance, so some businesses might choose to leave their systems unpatched. Customers should demand information on how their cloud providers are responding to Meltdown and Spectre and that whether the latest patches are in place.

IV. CLOUD SECURITY MODELS – A REVIEW

Vandana et al [1] introduced two technologies "Location-based-cryptography" and "Geo-Encryption algorithm" for providing security to the data access in the cloud computing for any particular location by using location-based encryption. For this to happen an anti-spoof GPS is required which provides very accurate location of the user for accessing data. Data stored on cloud can be given a Label. An Index table stores these label and refers to user's geographic location and timeframe.

Peng et al [2] has designed an architecture for securely storing the data in a multi cloud environment. This architecture make use of a symmetric key algorithm AES with 128 bits key size. An asymmetric algorithm, which is comparatively more secure but less fast, can, however, be used to manage keys of symmetric encryption. This algorithm makes use of data slicing policy to slice a file into many fixed size slices. Later the data distribution policy decides on which cloud a certain data slice should be stored. This approach has a drawback that it does not support video files and takes more time when the file size is large, since the file slice is of fixed size.

Navia Jose et al [3] has proposed a three-layer system structure in which each layer contributes its part for securing data. User authentication is taken care of by the first layer by using access control tools to check user authorization and also restrict unauthorized access to user data. The second layer is responsible for data encryption by using a fast and secured algorithm - AES. At this level, user privacy is also maintained, using fine-grained attribute based access control policies through access control policy algorithms. The third layer supports the faster user data recovery by using Byzantine fault tolerance algorithm methods. The three level structure ensures that the data is not tempered.

Subramanian et al [4] has proposed an architecture which specifies that the application data (files and databases) is partitioned and distributed to distinct clouds. This architecture makes use of Advance Encryption Standard (AES) with the key size of 256 bits, for data protection. Here two clouds (cloud A and cloud B) are used for storing the files such that one cloud stores one half of the file and the other cloud stores the other half. There is also one private cloud for storing the metadata of the files such as secret keys, passwords and encrypted access paths. In this approach, if a service provider conspires, then data breach threat is possible. Also this scheme will have a compute intensive decryption process since file access paths have to be periodically updated.

Sh. Ajoudanian et al [5] has enhanced the Open Security Architecture (OSA) provided free framework, to a new model for data security in cloud computing. It insists that the cloud should include a denial of service (DoS) protection. So the proposed framework has three layers. First being the virtual machine layer, second layer being that of Cloud

storage, pooling various resources from many external cloud providers. The last layer is virtual network monitor layer, which combines of hardware and software resources in a virtual system. The cloud security alliance provider should ensure that only the authorized users can access the clouds and should explain the techniques for the same.

Fabian et al [6] has designed a multi-cloud architecture that enforces the role-based access control mechanism based on the cipher text policy attribute-based encryption (CP-ABE). In CP-ABE, the encrypting party combines the encrypted data with an access control policy, which ranges over user attributes and defines who can decrypt them. It also makes use of Shamir's secret-sharing scheme and Rabin's Information Dispersal Algorithm for encryption and decryption. The main drawback of this scheme is that user revocation is compute intensive and also a standard procedure is not used to protect the keys.

D. Manivannan et al [7], proposed a symmetric – key encryption technique, popularly known as TSFS (transposition, substitution, folding, and shifting) algorithm, which includes transpositions and substitutions. TSFS uses three keys for additional security. Encrypting the database, particularly the data stored in memory helps to maintain confidentiality and protects data. For mutual transmission, synchronizer is used to store all the keys and the client system uses this key to decrypt the shared data. An enhanced TSFS is also proposed, which can encrypt the data that contains alphanumeric and few special characters to provide better security. Although it imposes few constraints on the data size and the special characters used. Also with increased number of keys, the processing and computation also increases.

Mazhar et al [8] has designed this architecture mainly to counter the insider threats. This methodology makes use of a cryptographic server (CS), which is a trusted third party and is responsible for access control, key management, encryption and decryption. CS generates a shared secret key and divides the key into two parts such that a single part cannot generate the other part. Since in this architecture most of the operations are being maintained by a third party service provider, it does not deal with all the other security issues.

We can collaborate our study in the following table that discusses various approaches, their contributions and drawbacks.

Table 1. Existing Approaches for Data Security

S. No.	Cloud Storage Security Techniques		
	Techniques	***Contribution***	***Drawback***
1	Improve Security of Data Access in Cloud Computing using Location [1]	Uses anti spoof GPS and includes "Location-based-cryptography" and "Geo-Encryption algorithm" for enhancing the security	Location based encryption requires more processing due to constant updates about the user location changes
2	Slice-based Secure Data Storage in Multi Cloud Environment [2]	A multi cloud AES based technique to provide security. Its data slicing policy slices a file into many fixed size slices.	Large files may take more time to get sliced due to fixed slice size. Also it does not support video files.
3	Data Security Mode Enhancement in Cloud Environment [3]	Three layer security model, first for strict user authorization, second for maintaining user privacy using ABE, third layer for user data recovery	This system is not fully automated and the network security is not unfocussed upon.
4	Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach [4]	It's a multicloud architecture using AES, two clouds are used, each storing one half of the file/s. One private cloud stores all the metadata and secret keys.	In this approach, if CSP conspires, then data breach is possible also decryption is compute intensive as file access paths have to be constantly updated.
5	A Novel Data Security Model for Cloud Computing [5]	Three layer architecture emphasizing on protection against DoS attacks. First layer has virtual machine, second has cloud pool, last layer has virtual network monitor.	Other than protection, integrity and confidentiality, other aspects remain untouched.
6	Collaborative and secure sharing of healthcare data in multi-clouds [6]	Multicloud architecture using CP-ABE based access control,	No standard procedure to protect cryptographic keys and User revocation needs heavy computation
7	Lightweight and Secure Database Encryption using Tsfs Algorithm [7]	Uses TSFS to protect data & databases. Uses three keys for enhancing security. For mutual transmission, synchronizer is used to store all keys.	Additional keys increases the processing and computation.
8	Secure Data Sharing in	Focuses on dealing with	Trust issues rise with the third

	Clouds [8]	insider attacks, makes use of third party cryptographic server for access control, key management, key generation.	party cryptographic server. Other security concerns are not taken care of.

V. CONCLUSION AND FUTURE SCOPE

Thus we have analysed various proposed models for making the cloud storage more secure. We have also discussed about the contributions and drawbacks in their proposed models. However, there are still major security concerns which lie undealt like external Cloud service provider's access control, network security and key management.

REFERENCES

[1] G. Vandana T. et al, "*Improve Security of Data Access in Cloud Computing using Location*", International Journal of Computer Science and Mobile Computing, Vol.**4** Issue.**2**, February-**2015**.

[2] P. Xul, et al, "*SSDS-MC: Slice-based Secure Data Storage in MultiCloud Environment*", In the Proceedings of the 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE 2015) pp. **304-309**, **2015**.

[3] N. Jose, C. Kanmani A, "*Data Security Mode Enhancement in Cloud Environment*", Journal of Computer Engineering Vol. **10**, Issue **2**, **2013**.

[4] V. R. Balasaraswathi, S. Manikandan, "*Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach*", In the Proceedings of the 2014 IEEE Advanced Communication, Control and Computing Technologies (ICACCCT 2014), pp. **1190-1194**, **2014**.

[5] S. Ajoudanian, M. R. Ahmadi, "*A Novel Data Security Model for Cloud Computing*", International Journal of Engineering and Technology, Vol.**4**, No.**3**, June **2012**.

[6] B. Fabian et al, "*Collaborative and secure sharing of healthcare data in multi-clouds*", Information Systems, Vol. **48**, pp. **132-150**, **2015**.

[7] D. Manivannan, R. Sujarani, "*Light Weight and Secure Database Encryption using Tsfs Algorithm*", In the Proceedings of the Second International Conference on Computing Communication and Networking Technologies, Karur, pp. **1-7**, **2010**.

[8] Mazhar Ali, et al, "*SeDaSC: Secure Data Sharing in Clouds"*, Systems Journal, IEEE pp **1-10, 2014.**

[9] V. Negi, M. Kalra, "*Optimizing Battery Utilization and Reducing Time Consumption in Smartphones Exploiting the Power of Cloud Computing*", In the Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), New Delhi, **India**, pp. **865-872, 2012**.

[10] V. Negi, M. Kalra, "*Framework for energy saving in the Android smartphone*", 2013 2nd International Conference on Information Management in the Knowledge Economy, **India**, pp. **161-165**, **2013**.

[11] J. Gantz, P. Miller, "*The Salesforce Economy: Enabling 1.9 Million New Jobs and $389 Billion in New Revenue Over the Next Five Years*", IDC Whitepaper, IDC #US41691316, **September 2016**.

[12] L. Goasduff, C. Pettey, "*Worldwide Public Cloud Services Market to Grow 18 Percent in 2017*", Gartner Press Releases, Stamford, **February 22, 2017**.

[13] J. M. Brook, et al, "*The Treacherous 12 - Top Threats to Cloud Computing and Industry Insights*", Cloud Security Alliance, **2017**.

[14] R. V. Dharmadhikari, et al, "*Cloud Computing: Data Storage Protocols and Security Techniques*", International Journal of Scientific Research in Computer Science and Engineering, Vol.**6,** Issue.**2**, pp.**113-118**, **2018**.

[15] Yogita G. Patil, Pooja S. Deshmukh, "*A Review: Mobile Cloud Computing: Its Challenges and Security*", International Journal of Scientific Research in Network Security and Communication, Vol.**06**, Issue.**01**, pp.**11-13**, **2018**.

Authors Profile

Ms V Negi pursed Bachelor of Technology from Punjab Technical University, Jalandhar in 2008 and Master of Technology from Panjab University in year 2013. She is currently working as Assistant Professor in Department of Computer Engineering, NMIMS, Navi Mumbai. She has published research papers in reputed international conferences including IEEE and Springer and these are also available online. Her main research work focuses on Cloud Computing, Cryptography Algorithms, Cloud Security and Privacy, IoT and Computational Intelligence based education. She has 8 years of teaching experience.

