International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT1833773

Case Study of Cloud Computing Security and Emerging Security Research Challenges

Shvetkumar Patel [*1], Apeksha Pavasiya[2], S. Gomathi[3]

[*1]Concordia Institute for Information System Engineering, Concordia University, Montreal, Quebec, Canada
patelshvet@gmail.com[1]

[2] Concordia Institute for Information System Engineering, Concordia University, Montreal, Quebec, Canada
apeksha5589pavasiya@gmail.com[2]

[3]Teaching Consultant UK International Qualifications, Ltd., Coimbatore, India
[3]mailtogomathisrinivasan@gmail.com

Article Info

Volume 6, Issue 5

Page Number: 83-93

Publication Issue :

September-October-2020

Article History

Accepted : 02 Sep 2020

Published : 20 Sep 2020

ABSTRACT

In this technological era, cloud computing is bombarded with immense benefits that includes availability, flexibility, ubiquitary access, and cost effectiveness. Cloud Computing offers its services to different kinds of users with the help of the World Wide Web on the virtual platform regardless of devices. Hence, all the resources kept on the same-shared storage device, which will lead to a considerable rise in various cloud security concerns for both; user and their private information. Data privacy can be compromised with a broad usage of cloud as smaller companies to bigger ones are adapting this versatile system. This paper examines several recent security attacks and proposed solutions of secure cloud computing from the perspective of organizations. Threat action varieties, other attacks with date, information exposed and number of record breach is presented with IT attack at risk. Finally, we have presented research challenges that can be worth noticing.

Keywords: Cloud computing and architecture, security challenges, real world cases, attacks, emerging challenges

I. INTRODUCTION

Cloud computing has made a tremendous effect on the Information Technology industry where the internet is handy. Cloud computing is replaced with traditional physical infrastructure of the storage in which there is no need to install servers, purchase of hardware, licenses and necessary software installation onto them. On that note, this idea brings the solution that is cost effective. With advancement of groundbreaking technology, physical arrangement of storage is giving a new way to virtual IT systems. Now, through web-applications, cloud service providers are finding several ways to provide an environment to access them. As an emerging trend, it offers numerous merits such as saving businesses' costs, mobility, security, disaster recovery, sustainability, increases collaboration, flexibility of work practices, and so on. That is why more

organizations prefer cloud- related services. When it comes to adapting, new technology enterprises are doing great job but they also have data privacy issues. In other words, [1] Information technology always comes up with the concerns of security and so cloud computing is; especially at the point when information can be accessed from anyplace over the internet makes prominent security apprehension. It clearly states that remotely accessible data are prone to major attacks. [2] Because of several benefits, hackers are also keen to find loopholes from cloud computing. This may create risks for the industries and comes more as a demerit where user's experience is mandatory. Today, one of the top challenges is the cloud computing security. There have been many real-world cases where it has been seen.

Based on the content mentioned above, this paper presents a summary of cloud computing along with the deployment model and service model, cloud computing related security challenges, and a potential solution that has been developed by an organization that makes sure that the incident will never occur in the future. The organization of this paper is as follows. Section II presents the **background**. Section III introduces the **details of attacks**, which are real-world scenarios where data of organizations were at risk and the effective solution. **Other** more **attacks** are presented in Section IV by type of breaches. Section V shows the **threat actions varieties**. Sections VI depicts the pie chart of **IT assets at risk**. Section VII addresses **the research challenges**. Section VIII **concludes** the paper.

II. BACKGROUND

Cloud computing is model that empowers on-request network access to a shared computing assets that are configured in a way that user requires less communication or management with cloud service providers. [3]

The Cloud computing model can be categorized into four deployment models that can be scale up or down as per the requirements, which are: [4]

A. Deployment Model

1) Private Cloud: Private cloud is a newly introduced term that is used by some vendors. It is the functionality similar to the intranet settled up within enterprises' data centre. Cloud resources are given to organization for private use. Only the company and assigned employees may operate a specific cloud. Eucalyptus Systems is an example of a private cloud [5].

2) Public Cloud: Public cloud is a kind of pay-per-use model; owned by a cloud service provider. They sell the resources and or part of resources to the end-user. It is less secure amongst all types. According to the usage requirement, it can be scale up and down. Microsoft Azure, Salesforce, Amazon, and Google lie under this category

3) Community Cloud: Community cloud is a kind of infrastructure shared by various organizations having the same interest. This may be operated either by them or by a third party. The banking sector or educational institute can use this type of model. Siemens IT Solutions and Face-book are examples of community clouds.

4) Hybrid Cloud: Hybrid Cloud is a private cloud; a mixture of two or more cloud infrastructure which can be any of private, public, or community clouds. It is managed centrally. It provides some extra features by which one can do some computation task without much of a stretch from private to a public cloud. Amazon Web Service (AWS) is an example of a hybrid cloud.

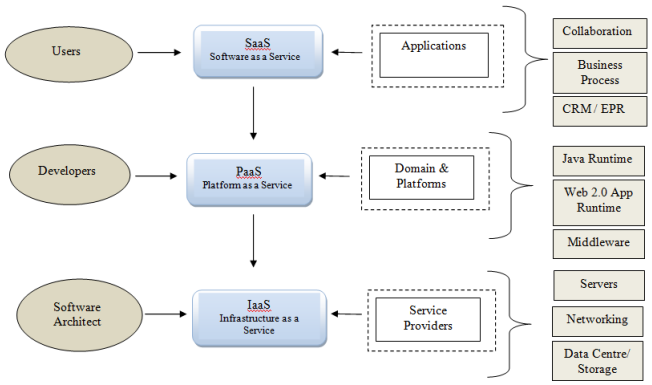


Fig.1 Cloud Computing Architecture and Service Delivery Model [6]

B. Service Model

Cloud Computing can be further divided into three parts based on the service offered by them.

5) Software as a Service (SaaS): In this service model, users can access data from anywhere without worrying about the pre-installation of software. One can access it via a web browser that makes this platform- independent. Google Apps is the best example of SaaS. It reduces the load of maintaining software, safeguarding and support. [7] The vendor is solely responsible behind managing server, operating system, database, and cooling.

6) Platform as a Service (PaaS): This service provides a platform especially for manager, end-user, or developers with high-level integration to try and run cloud application. Vendors mostly control excluding deployed application and in many cases, it may be the configurations as well. Microsoft Azure is an example of PaaS. It can be work as a pay-as-you-go methodology

7) Infrastructure as a Service (IaaS): In this type, a user of cloud can act as an administrator as they can operate the operating system. As per the name suggests, it provides the infrastructure alongside to Application Programming Language (API) company. It is the base of cloud computing. Cisco Metapod is an example of IaaS.

III.SECURITY CASE STUDIES

Diverse real-world circumstances where cloud computing and the habits in which the association reduce the event will be discussed. For each case the attack's type will be immediately delineated, the subtleties of the case will be presented. Besides, counteraction procedures will be inspected.

A. Account Hijacking

Account hijacking is a threat under which malicious attackers gain access to account's credentials which is highly sensitive information and that can cause compromise of these accounts [8].

In May 2019, Instagram (Chtrbox) has exploited. Instagram, an American company, is social networking service owned by Facebook, which allows users to upload photos and videos. The data on Instagram's database left open without any password that contain display pictures, followers, contact information like email and mobile number. Although financial information did not reveal in the breach, it gave access to geographical location and contact details that may not have meant to be public. Anurag Sen, security researcher, found out online database that holds 49 million Instagram users' data. Then he alerted TechCrunch, which found the owner to Mumbai-based Chtrbox, a social media influencer marketing agency that pays social media influencers to post sponsored content. It contacted some random people whose data was in the database and confirmed their personally identify able information, and they were connected to Instagram accounts, investigated by TechCrunch. Later, the stolen data was dumped and reportedly put for sale via Bitcoins [9, 10].

Prevention of this data breach requires the cloud to have a much more flexible environment from development to runtime. Though this method avoids the best security needs principle of slightest benefit,

passwords that cannot be crack-able would be best for assets, multi-factor authentication (MFA),regular key rotation and a bunch of other key practices that ought to be tenet. Given of critical discoveries, the businesses have knew their cloud accounts, workloads and container foundation. Without that, the organization is vulnerable to information crevices that stifle their ability to observe misconfigurations, unenforced approaches, or distinctive considerations that might simply result in a breach [11].

B. Traffic Flooding

Traffic flooding attacks bring a service or network down by sending a massive amount of traffic at a particular server. In other words, it stops responding to the legitimate request just because of bogus traffic, which is exhausting more resources. This attack creates network congestion [12].

In September 2016, OVH the telecom provider was hit by an attack which was a hundred times larger than most of its kind. The internet slowed down in the almost entire eastern United States.21 year's old college student from New Jersey along with his two friends initiated Mirai Botnet (Internet-connected device) into the world. Originally, they are trying to gain merit in the Minecraft, the computer game. VDOS was an advanced botnet: a network of malware-infected, zombie devices that its masters could commandeer to execute DDoS attacks at will. That was an updated version of the olderIoT zombie. It was entirely different from the normal DDoS attack. The new malware scanned the IoT devices that are using default security settings provided by the manufacturer as hardly any users have changed the default passwords. Surprisingly, it affected nearly 65000 devices within 20 hours and the number was doubling every 76 minutes and stands between 200,000 and 300,000 infections. This attack achieved a range of 50 gigabits per second that used to be 10 to 20Gbps [13].

As a solution, the FBI, industry researchers and network companies like Akmai created some honeypots, hack-able devices to analyse how infected "zombie" devices communicated with Mirai's command and controlled server. Later, Internet host OVH started providing service called VAC that was the mitigation tool for Minecraft DDoS attack. After that, the FBI worked with private-industry researchers and developed tools that can help them to track where traffic is diverting [13].

C. Wireless Local Area Network Attack

In wireless area, network attack attacker breaches into the authorized user's wireless area network and performs various attacks. For example, man-in-the-middle attack, cipher attack, denial of service attack (DoS), and flooding [14][15].

In November 2017, one person from the ground hacked hundreds of planes. By taking merit of a weak link in satellite's equipment, Ruben Santamarta peeked inside aircraft flying thousands of meters above him. Some of them are commercial flights operated by the biggest airline in the world. By hacking onboard systems, investigated Wi-Fi[16]and carried out surveillance on all passengers' devices that are connected. Due to vulnerabilities in antennas that are sending data to the modem, he was able to spy. He turned the satellite communication kit into "radio frequency weapons" [17].

The proposed solution for this attack can be many. Firstly, the use of firewall technology. That can be useful for analyzing the incoming and outgoing traffic and helps to decide whether to block traffic or allow based on some rules. Moreover, reduce AP signal strength disable SSID broadcasts are other feasible solutions [18].

D. XML Signature Wrapping Attack

In XML signature wrapping attack, application logic processed unmodified element and faked element together into the structure of the message and that is being injected by threat actors. And by doing this attacker acts as a genuine user and can access web service requests [19].

The second-largest U.S. based financial company called Capital One's information had been breached in July, 2019. In this breakthrough, customer's personal identification information was exposed such as social security numbers, birthdates, email addresses, bank account numbers and a great amount of credit card data on Paige A. Thompson's GitHub account from a rented cloud data server. The attack also affects 6 million Canadians' Social Insurance Numbers (SINs) and 100 million US consumers. While breaking the Capital One, Thompson used the anonymous TOR and VPN I predator as these tools are fool proof ways of covering tracks. Even if a Web Application Firewall (WAF) was deployed to guard the cloud, the breach has happened because the configuration of the firewall was not legitimately designed. After this breach Capital One allowed the FBI to detect the attack and informed the law enforcement about this data theft. Capital One fixed the configuration vulnerability and immediately began working with federal enforcement. Via a variety of channels, the company notified its users and make free credit monitoring and identity protection available to everyone [20].

Proposed solutions on this cloud attack are knowing your infrastructures well, an appropriate configuration of the cloud security appliance, and principle of least privilege and resource separation. After this incident, big to small enterprises must consider this breach as an alarming sign so that implications of failing security will not damage the organization's network and devices anymore or else they at least lessen the consequences. By limiting the access, user or an application should only be permitted to perform specific job roles. Capital One company should have stored and run their data from different places so that may not have been more liable to data breaches[21,22].

E. Malware Injection

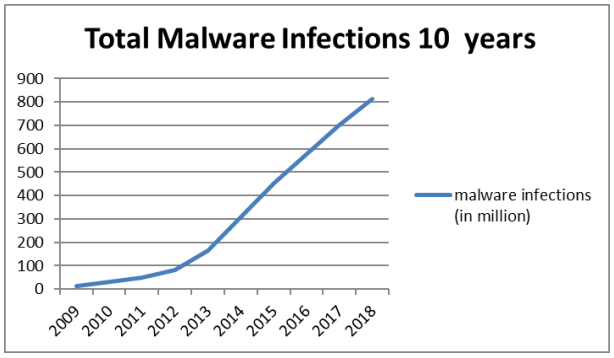
In malware injection, attack malicious server or virtual machine is being tried to inject by the attacker. By making its own malicious service implementation module, attackers try to add it to a cloud system. Then, the attacker has to act like to make it a valid service. After successfully doing so valid request of the user has been redirected to malicious service implementation and the code of the attacker starts its execution [23].

Malicious actors are now taking advantage of Amazon's cloud by hosting domain services and drive-by download sites. Besides, researchers have explored many domains that are being misused to install malware as in phishing campaign and spam on Amazon's cloud platform for stealing information such as banking credentials and other sensitive details [24]. This attack originated in Brazil and the purpose was to target Brazilians only and steal customers' data from nine banks. To increase its success rate, malware shut off the normal procedure of virus protection programs and plugins that could make the online banking system secure. Added that digital certifications and credentials of Microsoft Live Messenger were stolen by the malware [25].Apart from this, evil files downloaded on victims' machines from attack sites with the module, which pretend as root and disabled the anti-virus applications. These attacks originate in the same way that spamming campaigns works where users received emails with links and that redirects them to harmful sites, which leads to significant security concerns. During the hack, threat makers installed some components that include login information of nine Brazilian and two international banks. Besides, hackers managed to get eTokens that were part of an authentication routine

[26]. This attack was identical to previous hacks that have seen for years now.

A general solution for this cause is to use specialized anti-phishing software for handling cloud-based email communications. Most hackers are after your passwords, financial info, identity and money. Therefore, it is a prime step that should be implemented in order to protect business firms from phishing swindle. As a centralized system on a server, every host machine should have a defense system connected to the mail client. So that threats on the cloud mail system, spam emails and spear-phishing attacks could be easily detectable by that mechanism. Generally, these are implemented in a collaborative or individual virus protection program and connect to email clients such as Postbox, Inky, Outlook, Hiri, Notes, etc. Moreover, with detecting intrusions, it is mandatory that companies should come up with remedy related to cloud with full supervision of intrusion detection system. Use IDS (Intrusion Detection System) that recognizes the activity on network and then takes actions about the insiders' abnormal behavior. However, one should report to Amazon Web Services (AWS) for this kind of spiteful act. To handle AWS vulnerability assault, users can report to the website given here: (http://aws.amazon.com/security/vulnerability-reporting/). After this attack, AWS lowered down all the malicious links.

The line graph below addresses malware injections occurred between 2009 and 2018, a period of ten years:



In 2009, there were 12.4 million malware injection attacks happened, which was the least. Between 2009 and 2012, there has been seven times higher in the number of malware hacks. Over the same period, malware injections have gradually inclined up to 82.62 million in year 2012.

According to the chart, the malware injections in next years increased more rapidly. That number rose steadily to 165 million by 2013 and then sharply to 702 in 2017. At this point, the number of cases remained continuously growing until 2018.

F. Social Engineering Attack

Social engineering attack requires human interaction that tries on various users in a way that they can be part of a trick to break usual security measures and procedures [27][28].

Apple technical assistance gave access to an iCloud account to hackers unintentionally and Amazon tech support helped them to collect a bit of detail, the four digits of the credit card number. In other words, Amazon considers very four-figure non-essential in a user account that is enough to provide the whole picture on the internet are particularly identical which Apple contemplates shielded to carry out the personal evidence. The generation of cloud computing was at risk when information management flaws were exposed and the entire technical industry had faced endemic of this disconnect [29].The digital life of a person was at risk and he lost all his Gmail, Twitter and Apple ID information. As all these were interconnected with apple ID, the iCloud was also cracked.

There are multiple factors to be taken care of while using cloud storage and your data as follows:
-Avoid storing sensitive information in the cloud, using different passwords for different sites in a manner, which cannot be traced, and read

SLA(Service Level Agreement) to find out how cloud storage service works that can give you a better idea what a person can store and what cannot be stored in cloud.

-Secure your devices with the anti-malware software, firewalls, and email filters of recent edition. Consider the VPN.

-Backup regularly to an external hard drive

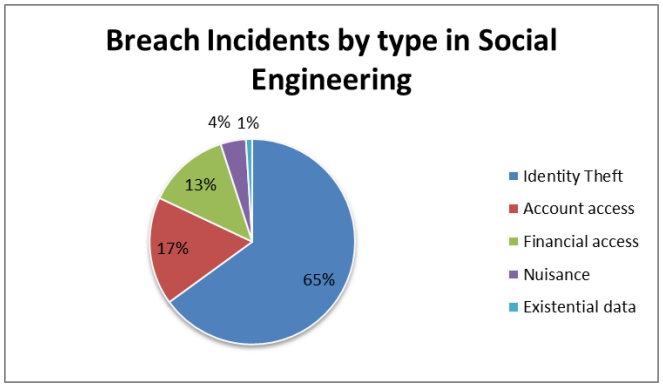
-Due to alack of awareness among humans, they became the weakest link for this type of attack hence they need to train.

-In recent years, social media sites are booming with too much-shared information of human-beings that can legalize attackers to speculate passwords or extract industries' privileged data through posts. Awareness in secure usage of a system is the pointer to prevent such happenings.

-Always, prefer to maintain two-factor authentication to secure your account from unauthorized access or third party access.

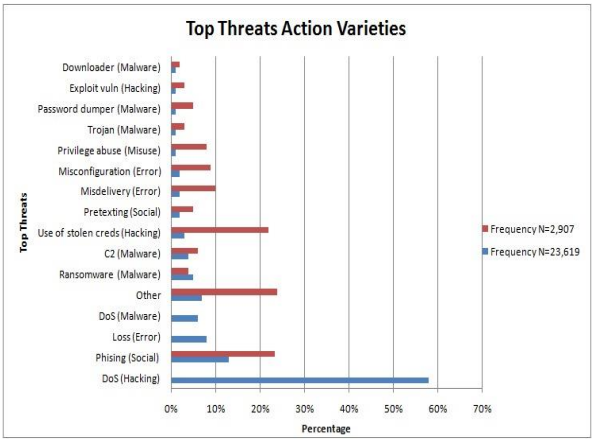
-Change password and access frequently with irregular intervals [27].

The below pie chart illustrates the social engineering breaches in various ways as identity theft, financial access, nuisance and so on:



At first glance, it is evidently shows that the main reason of the social engineering attacks is identity theft at two-thirds, while in the smallest amount through existential data. Apart from this, account and financial access are the factors in breach incidents makes an appearance of 17% and 13% consequently. In addition, nuisance in social engineering knows 4% of incidents.

IV.THREAT ACTION VARIETIES



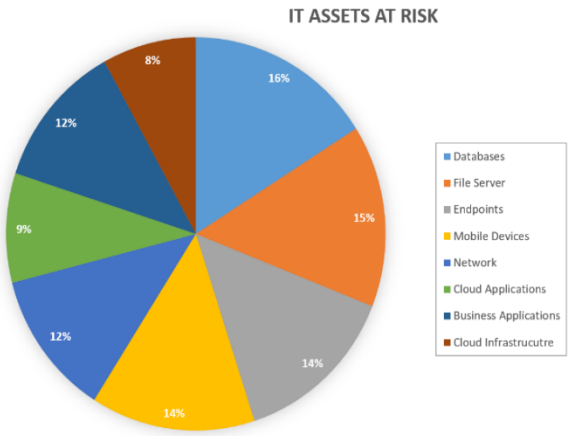
Making a look at danger move varieties permits us to dive somewhat deeper into the hacker's tool compartment. Figure 2 gives a thought of what activity varieties drive incident numbers. Surprisingly, Denial of Service (DoS) is covering a large part. We additionally observe a decent piece of phishing, however since information revelation could not be affirmed, they remain occurrences and do not graduate to break status (yet perhaps they can in the event that they take several midyear classes).Overall in 6th , we see ransom ware springing up like a helpless connection requesting cash—in many cases, they get. "Other" speaks to any count not represented by one of the classifications in the figure. It turns out there are lot of breaches (675 to be explicit) that did not contain any of the top varieties.

V. OTHER ATTACKS

Type of Breach	Name of Company	Number of records breached	Information exposed	Date
Financial Data Breaches	Capital One	106 million	Name, Contact number, addresses, email-id, birthdates and self-reported income, information related to credit card, history of payment	22/03/2019
	Evite	100 million	Name, email-id, passwords, and IP addresses of customers.	22/02/2019
	DoorDash Breach	4.9 million people potentially affected	Names, email-id, delivery addresses, contact numbers, and hashed and salted passwords	04/05/2019
	American Medical Collection Agency	20 million	Social Security numbers, Birth dates, payment card data, and credit card information.	01/08/2018, to 30/03/2019
	Zoll Medical	277,319	Patient names, addresses, date of birth, Social Security numbers, some medical information	From 08/11/2018 to 28/12/2018
Education Data Breaches	Georgia Tech	1.3 million	Names, addresses, Social Security numbers and date of birth	14/12/2008 to 22/03/2019
	Federal Emergency Management Agency (FEMA)	2.3 million	Street addresses, financial institution names, electronic funds transfer numbers, and bank transit numbers of survivors of hurricanes Harvey, Irma, and Maria, and the California wildfires.	15/03/2019
	Palm Bay, Florida	Up to 8,500	The billing information of residents who uses the portal to pay their utility bills	29/08/2019
Healthcare Data Breaches	SingHealth	1.5 million patients records	Name, NRIC number, address, gender, race and date of birth	04/07/2018
	UnityPoint	1.4 million records	Name, address, medical data, Social Security Number, treatment information, payment card and insurance details	14/03/2018 to 03/04/2018
	Virtua Medical Group	More than 1065 individuals	Patient's name, Physician's name, birth dates, 462 patient's doctor's letters and medical notes	21/01/2016
Other Business Data Breaches	BioStar 2, a Suprema-based security platform	28 million	Fingerprint data, facial recognition data and face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, personal details of staff.	05/08/2019

VI. IT ASSETS AT RISK

The chart describes insecurity on the information technology resources such as mobile devices, network, database, cloud applications and so on. Databases are highly at risk in terms of cloud computing security service whereas cloud infrastructures has minimal possibility.



From the pie chart it is clear that the majority of endangerment is on databases (16%), file servers (15%). Nearly mobile devices and endpoints are at third position with the same amount of risk of 14%.Applications run on cloud accounts for nine per cent of risk in technological asset. Subsequently, 12% chances of risk in business applications and network. Cloud Infrastructure is at 8% on threat level, which is the lowest in all the information technology assets.

VII. RESEARCH CHALLENGES

Cloud computing research indicates the challenges of meeting the requisites of cutting edge private, public and hybrid cloud computing architectures, in addition to the difficulties of permitting applications and development platforms to take the benefits of it.

The examination of cloud computing is still at the beginning phase. Many existing issues have not completely tended to, while new difficulties keep rising out of industry applications. A portion of the difficult research issues in distributed computing are given underneath: [31, 32]

A. Portability

The capacity to move the application and its information starting with one spot then onto the next. It could be accomplished by limiting conditions on the fundamental air is called Portability. Information and applications are the compact segments that could be moved and re-prepared paying little mind to the

supplier, working framework, area, stage, stockpiling, and so forth. For instance, if the old cloud condition is Windows and another cloud condition is Linux then an application running on the old cloud would have the option to run on another cloud without being changed.

More often than not, convenience is referred to as to a great extent needed to alleviate merchant lock-in, however moving starting with one framework then onto the next with a base exertion, as might be conceivable with holder administrations, can likewise improve strength and scalability[33].

B. Interoperability

Past trust and security, the interoperability between cloud is a tremendous test for the drawn out reception of cloud computing. This empowers at least two frameworks to cooperate to exchange information and utilize that information. The majority of the open cloud networks are not planned such that they can't do communication with other cloud organizations and designed as a shut framework. This makes substantially more troubles in networks so as to join endeavours' IT frameworks, acknowledge profitability gains and cost investment funds [35][36]. In this way, the business' administration level of understanding must assist cloud with overhauling gives to make interoperable stages to creating and allowing the versatility of information. Notwithstanding, cloud administration classifications will have particular interoperability challenges and that is the most genuine undertaking to deal with than interfacing administration to far off capacity. Should associations think about conduct interoperability as an unsafe undertaking to keep up? Are there some other approaches to accomplish information between operability in far off capacity?

C. Access Control

IT resources are executed and utilized by rules, guidelines of Information Technology administration, which ensure resources utilized in supporting procedures of an organization are very much overseen, and furthermore it should give guarantee of ensured regulations. Authentication and personality the board is indispensably significant than at any other time. What are the methods of resetting a password? What is the required level of password strength? Does the change in frequency make service provider invoke? What is the password recovery method with that particular account type? Above all asked questions have implemented already in internal systems and data security aspects. With the usage of strong passwords and typical security procedures, one would be able to safeguard that element of access.[37]

D. Security

In the beginning phase of distributed computing, security has been a principal issue and now with the rising century of innovative age it is prime to take a gander at. As should be obvious where genuine information is being put away and how it measures the transmission while retrieval. For clients, the security of information put away in cloud is the central obstruction as protection imperfections are diminished, and the accessibility of contemporary methods are expanded for programmers. As a result, when con artists hack the cloud framework it got scattered. In like manner, endeavours ought to have made their structures and applications private with significant and versatile security components. How might the cloud framework respond when assaults happened? While utilizing distributed computing security highlights, on what premise undertakings fabricate trust among clients and their framework.

E. Limited Scalability

The scalability of the cloud layer is characterized as growing the limit of the gave programming service. Cloud figuring specialist organizations guarantee to hand over a plentiful measure of adaptability to users. Millions of consumer are making strides towards the cloud for putting away their information, yet

specialist organizations can't satisfy their elevated standards. Thus, issues in inferring ideal cure in the accessibility of the distributed storage lead to another significant examination zone [32].

VIII. CONCLUSION

Cloud computing is an emerging techno-savvy that uses a virtual environment to execute and perform tasks globally. Big businesses are highly dominated by the cloud environment and taking a major shift to cloud computing services whereas some of them are in competitions to build their private cloud services. In which, many organizations are failing to get to the bottom of services provided by the cloud. Hence they end up delivering secretive information in danger and the chances of losing data and its privacy will be more and then cloud security comes into the picture. As a result, attack take place straightforwardly into web services and victim's devices. As we have represented some of the recent cyber-attacks on cloud computing that need to be forced by big to small companies. Also, indicated some solutions for the same with several factors affecting it. Therefore, their firm will remain protected. There are various challenges faced by consumers in cloud computing that need profound research.

IX. REFERENCES

[1]. A. Subashini S. and Veeraruna K. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[2]. Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).

[3]. Peter Mell, Timothy Grance, ―The NIST Definition of Cloud Computing‖, Jan, 2011. http://docs.ismgcorp.com/files/external/DraftSP-800-145_cloud-definition.pdf

[4]. V. Jain, V. Sharma. Surveying and analyzing security challenges and privacy in cloud computing. International Journal of Computer Science and Information Technology & Security, vol. 3(5), 2013, pp. 316-321.

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

[6]. M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. ―What's Inside the Cloud? An Architectural Map of the Cloud Landscape.‖IEEEXplore, pp 23-31, Jun. 2009.

[7]. R. Maggiani, Communication Consultant, Solari Communication, ―Cloud Computing is Changing How we Communicate‖, 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[8]. Cloud Security Alliance, "Top threats to cloud computing", Assets Extrahop , August 2019. Available: https://assets.extrahop.com/pdfs/analyst-reports/CSA-Cloud-Computing-Top-Threats.pdf

[9]. U Verma "instagram data breach" Available: https://www.businesstoday.in/technology/news/instagram-data-breach-mumbai-based-chtrbox-leaks-private-data-of-social-media-influencers/story/348915.html

[10]. J. Lirk "Database May Have Exposed Instagram Data for 49 Million" Available: https://www.bankinfosecurity.com/database-may-have-exposed-instagram-personal-data-a-12503

[11]. C. Pedigo "The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020" Available: https://www.lacework.com/top-cloud-breaches-2019/

[12]. York, D. (2010). Control Channel Attacks. Seven Deadliest Unified Communications Attacks, 71–92. doi:10.1016/b978-1-59749-547-9.00004-1

[13]. G. Graff "How a Dorm Room Minecraft Scam Brought Down the Internet" Available: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

[14]. M. Sri Lakshmi, Dr. S. Kumar - A Review on Wireless Network Attacks et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2540-2542.

[15]. Soni M., Rajput B.S., Patel T., Parmar N. (2021) Lightweight Vehicle-to-Infrastructure Message Verification Method for VANET. In: Kotecha K., Piuri V., Shah H., Patel R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 52. Springer, Singapore. https://doi.org/10.1007/978-981-15-4474-3_50

[16]. M. Soni, A. Jain and T. Patel, "Human Movement Identification Using Wi-Fi Signals," 2018 3rd International Conference on Inventive Computation

Technologies (ICICT), Coimbatore, India, 2018, pp. 422-427, doi: 10.1109/ICICT43934.2018.9034451.

[17]. T. Brewster "This Guy Hacked Hundreds Of Planes From The Ground" Available: https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/#38b0e08b46f2

[18]. Suroto – "WLAN Security: Threats and Countermeasures" International Journal On Informatics Visualization, vol 2 (2018) no 4

[19]. S. Gajek, M. Jensen, L. Lioa and J. Schneck, "Analysis of signature wrapping attacks and countermeasures", IEEE International Conferenceon Web Services, 2009.

[20]. C. Pedigo "The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020" Available: https://www.lacework.com/top-cloud-breaches-2019/

[21]. N.Hazut "Capital One Breach: How It Could Have Been Prevented" Available: https://www.securitymagazine.com/articles/90832-capital-one-breach-how-it-could-have-been-prevented Aug,2019

[22]. H.Poston "Lessons learned: The Capital One breach" Available: https://resources.infosecinstitute.com/lessons-learned-the-capital-one-breach/#gref. Oct, 2019.

[23]. R. Rao, Vaudha, S. Bhat-International Journal of Innovative Research in Computer and Communication Engineering. Vol. 6, Issue 4, April 2018

[24]. D.Fisher "Attackers Using Amazon Cloud to Host Malware" Available: https://threatpost.com/attackers-using-amazon-cloud-host-malware-060611/75306/ . Jun, 2011.

[25]. V. Zakorzhevsky "Monthly Malware Statistics" Available: https://securelist.com/monthly-malware-statistics-june-2011/36360/. June,2011.

[26]. D. Bestuzhev "Financial data stealing Malware now on Amazon Web Services Cloud". Available: https://securelist.com/financial-data-stealing-malware-now-on-amazon-web-services-cloud/30647/. Jun,2011.

[27]. I. Kotenko, M. Stepashkin, and E. Doynikova, "Security analysis of information systems taking into account social engineering attacks", IEEE 19th International Eurimicro Conference on Parallel, Distributed, and Network-Based Processing, 2011.

[28]. Soni M., Patel T., Jain A. (2020) Security Analysis on Remote User Authentication Methods. In: Pandian A., Senjyu T., Islam S., Wang H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018). ICCBI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31. Springer, Cham. https://doi.org/10.1007/978-3-030-24643-3_60.

[29]. https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ Jun,12.

[30]. N.Lord, "Social Engineering Attacks: Common Techniques & How to Prevent an Attack".Available: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack .Jul,2019.

[31]. Rabi Prasad Padhy, ManasRajanPatra and Suresh Chandra Satapathy, ―Cloud Computing: Security Issues & Research Challenges‖, IJCSITS, Vol. 1-No.2, December 2011, pp. 136-146.

[32]. W.K. Chan, Lijun Mei, and Zhenyu Zhang, "Modeling and testing of cloud applications", to appear in Proceedings of2009 IEEE Asia-Pacific Services Computing Conference (APSCC 2009), (Singapore, December 7-11, 2009), IEEE Computer Society Press, Los Alamitos, CA, USA, 2009.

[33]. D. Sheppard. " Cloud interoperability and portability – necessary or nice to have?"Available: https://insightaas.com/cloud-interoperability-and-portability-necessary-or-nice-to-have/. Nov,2017.

[34]. O. Diez, A. Silva- Reliability issues related to the usage of Cloud Computing in Critical Infrastructures. Available: https://core.ac.uk/download/pdf/148661056.pdf

[35]. M. Bollinadi V.Damera- Cloud Computing: Security Issues and Research Challenges. Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org Volume 7, Issue 11, November (2017).

[36]. M. Soni and T. Patel, "Systematic investigation on LargeScale simulations in big data systems," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 684-688, doi: 10.1109/ICISC.2018.8398885.

[37]. M. Soni and A. Jain, "Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2018, pp. 539-543, doi: 10.1109/ICCMC.2018.8487887.

Cite this article as : Shvetkumar Patel, Apeksha Pavasiya, S. Gomathi, "Case Study of Cloud Computing Security and Emerging Security Research Challenges", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 5, pp.83-93, September-October-2020. Available at

doi : https://doi.org/10.32628/CSEIT1833773

Journal URL : http://ijsrcseit.com/CSEIT1833773