Investigation of Cloud Computing Security Issues & Challenges

Abhishek Sharma[1,*] Umesh Kumar Singh[2]

[1] *Department of CSE, MIT, Ujjain, India*
[2]*Institute of Computer Sciences, Vikram University, Ujjain, India, umeshsingh@rediffmail.com*
**Corresponding author. Email: abhiujn9@gmail.com*

ABSTRACT

The Trends of using cloud computing in IT industries is increasing since the Inception of this innovative technology. This new shift in the industrial technology, which will grow and develop continuously their e-governance in the coming few years. Most of the enterprises are migrating towards the cloud-computing environment rapidly due to its various advantages over traditional one. As per cisco, more than 93% workloads will be processed by Cloud data centers in 2021. Even several republics have already initiated to shape their own governmental public cloud around the globe. Phishing attempts affected the majority of educational establishments (60 percent) and account compromise (33 percent) in 2020. According to Gartner, consumers are responsible for more than 95 percent of cloud security flaws. Increasing frequent cyber-attacks potentially cause significant material damage if no special security measures are taken. The objective here is to investigate the security issues & challenges in terms of cloud specific vulnerabilities & threats using real time experimental setup with vulnerability scanner which further provide an ease to applications deployment.

Keywords: *Cloud Computing, Cloud Platform, Data breaches, Security Threats, Security Vulnerability.*

1. INTRODUCTION

The key profits of cloud computing is high flexibility and scalability in organizational resources for meeting excellent reliability, peak time demand and availability of assets can be used at all-time, from everywhere, with zero cost for managing and installing the h/w & s/w infrastructure. 24x7 infrastructure availability is the basic requirement of the commercials & government organization to meet & to implement e-Governance with a minimizing downtime. Cloud Computing denotes to applications, platform & infrastructure delivered as services with the help of Internet, h/w and systems s/w in the data-centers which are responsible for these services. Security is a leading concern if an enterprise shares their critical information to geologically discrete cloud platforms. A Cloud Services Provider (CSP) is supposed to control over computing system infrastructure, when the enterprise migrates to consuming public cloud-services. Hence, such establishments may lose command over how they protect their computing environment and they may be worried with the respective confidentiality and safety as the novel technology which is a main source of new vulnerabilities.

The previous methods investigated various types of cloud computing tools/models, and as a result, suggested a vulnerability assessment conceptual model for Cloud computing constructed on the CVSS 2.0/3.0, & is produced or available by the NVD on a regular basis. Because the provided prototype/procedure is based on security mechanization protocols for CC. It has capacity to automobile & interoperate with additional current implementations and prototypes, as well as handle all potential cloud vulnerabilities that have yet to be uncovered. It deals with vulnerability concerns using CVSS, which adds new aspects to the effective management of undiscovered vulnerabilities [1]. Vulnerabilities are faults or weaknesses in a system that might lead to a cyber-attack. Potential enemies identify and exploit these flaws in order to get access to the network. Vulnerabilities include injection, cracked authentication, private records exposure, XML Exterior Objects (XXE), and destroyed access control. Vulnerability assessment is a technique for identifying possible flaws in a system or network. Penetration testing entails a vulnerability evaluation as well as proof of the testing methodology' effectiveness. Pen testing employs both human and robotic procedures to mimic a system assault, while Vulnerability Assessment depends solely on automation tools. Vulnerability Assessment will be utilized to integrate with an institution's risk & vulnerability management platform, and it can automate thousands of security tests. These are the benefits of vulnerability analysis. The downsides of automated program are that they might produce a large number of false positives and an excessive quantity of data. Second, it is unable to detect logical attack routes such as password reuse. The third point is that Vulnerability Assessment solutions are often generic and based on the tool's results [31-34].

Penetration testing also has other advantages, such as taking security mitigation mechanisms into account, looking at vulnerabilities identified to provide a complete picture of the concerns, and avoiding false positives. Secondly, it is unable to detect logical attack routes such as password reuse. The third point is that Vulnerability Assessment solutions are often generic and based on the tool's results. Whereas drawbacks include the fact that it may lonely be conducted through qualified pen testers, thus without an in-house pen tester, businesses hire an external firm for penetration testing, and it requires additional time, energy, and money than vulnerability assessments [2].

The goal of this project is to look at security concerns and challenges related to cloud based vulnerabilities and threats utilizing a real-time experimental design with a vulnerability scanner & penetration testing that makes application deployment easier. Significant security concerns and difficulties linked to the virtual machine are investigated and discussed. The origins of cloud vulnerabilities are also addressed, which aids in the discovery and analysis of security risks. In the future, risk assessment and analysis can be done utilizing vulnerabilities to safeguard the cloud from hackers.

2. RELATED WORK

Cloud Computing is nothing however virtual asset management for data center assets that are stored in software generated pools. This clarification just scratches the top layer of the capabilities of cloud-based services. Solutions can provide on-demand computing services to collaborated organizations over the internet through apps, allowing them to retain data and processing power on a per-activity basis. According to NIST [3], a cloud model involves three service models, four implementation models, and five basic characteristics, or will say it’s a 3-4-5 reference model. Each service model is devoted to nourishing varieties of business needs. Among three main service models, first is SaaS, second is PaaS & third is IaaS. Software as a service (SaaS) provides apps which can be retrieved through the internet. Platform as a service (PaaS) provides a cloud-based background to users for structuring and delivering applications. Infrastructure as a service (IaaS) provides infrastructure like storage facilities, networks, servers, etc. on demand and through the web [4]. Apart from the models there are mainly four cloud actors participate in the computing cloud provider, consumer, carrier, auditor [5]. According to the commonly established designation of cloud computing given by the NIST, there are four primary deployment models: public, private, hybrid, and community deployments. The 3-4-5 reference model of Cloud can be stated as follows:

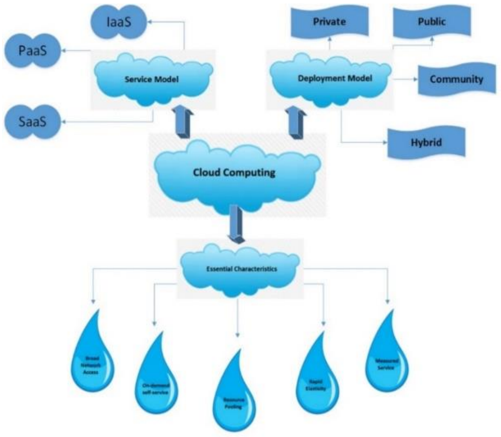


Figure 1 Reference Model of Cloud Computing (Source: NIST)

The purpose of this article is to help identify those points in the application lifecycle when vulnerability scanning may be done and to provide useful information for better protecting cloud applications. Finally, this paper analyses and shows that orchestration of vulnerability scanning tools can help to increase vulnerability detection coverage [6]. The author's major objective in [7] is to provide an answer to the topic of how to evaluate vulnerabilities in cloud computing and what the most common penetration testing techniques are in cloud settings. In [8], author presented a taxonomy for security testing approach categorization, which includes three primary categories at level 1 (identification, testing, and reporting), eight security testing methods at level 2, and nine categories at level 3, such as black-box testing and risk assessment. Based on the methodology adopted for the study. The author in [9] define a consistent taxonomy for security needs, threats, vulnerabilities, and responses in order to carry out the suggested end-to-end mapping. It also emphasizes security issues in other domains such as trust-based security models, cloud-enabled Big Data apps, IoT, SDN, and Network Function Virtualization (NFV).

The primary objective of the author in [10] is to define a consistent taxonomy for security needs, threats, vulnerabilities, and responses in order to carry out the suggested end-to-end mapping. Using an agent-based model, provides a methodology for identifying cyber security threats in the construction sector and analyses the vulnerability of traditional and hybrid delivery methods (ABM). That is, the susceptibility of various project team members and development bodies as a result of Construction 4.0 at various stages of the construction life cycle. The findings of this study aid in the identification of possible hazards and offer a foundation for evaluating the impact of interactions in a digital world among project team members. The suggested ABM technique will be fully investigated in future study, with the goal of extending that to other project delivery procedures & data sharing networks in building projects [11]. The author's major objective in [12] is to describe a system that can continuously monitor and analyze for vulnerabilities in cloud-deployed apps as part of the ongoing iteration and continuous delivery process. The SDLC should include a mechanism for testing for vulnerabilities following each application upgrade. Author [13] identifies that all of these protection techniques for various assaults are not successful for all attacks and can only be stopped to a certain extent after the comprehensive examination of various attacks and their prevention methods. In the case of an insider assault, the cloud administration must work correctly, but in the case of a worm or DDoS attack, it must ensure security among cloud customers. The authors of [14] give a detailed security study of CC-enabled IoT and the current state-of-the-art in the research domain through a survey. Finally, open concerns are discussed as well as future research work and prospective areas of application and consideration. It outlines the many CC security, privacy, and trust techniques depending on various criteria. In [15], the authors explain RDFI methods as a software application called CloudStrike, which includes different chaos engineering algorithms. CloudStrike has been tested against architecture hosted on AWS and GCP, two prominent public cloud infrastructure providers. Time performance rises in a linear relationship with rising assault rates. In addition, the study of vulnerabilities discovered by security fault injection was utilized to enhance the security of data centers, demonstrating the efficacy of CloudStrike's security intelligence. As a result, we believe that our techniques are appropriate for addressing current cloud security concerns. The authors of [16] discuss their research on cloud and edge security issues and demands, as well as known threats and vulnerabilities.

The goal of this article is to look into the many aspects of cloud and edge computing, as well as the current privacy and security concerns that these schemes face. The author then offers a new classification of contemporary security approaches used in these sectors. This investigation examines several security risks to cloud and edge computing services, as well as unresolved concerns and future approaches 31-35].

3. CLOUD COMPUTING EXPERIMENTAL SETUP

The experimental setup was done using open source cloud service provider. Open stack platform is one of them which have to be evaluated through the study [17-20]. Cloud computing layered model is very significant with the intentions to offer assistances for smaller direct investing in assets during deployment, greater scale-up, lesser functional expenses, easiness of access over the Web, decreased commercial risks and maintenance expenditures. Infrastructure layer consists of compute processor, block storage, network whereas platform layer includes runtime, OS, queue, database, object storage, identity Management Services and the application layer incorporates various apps like LMS, monitoring, CMS, communication, finance applications, collaboration, CRM and many more. [35-39]

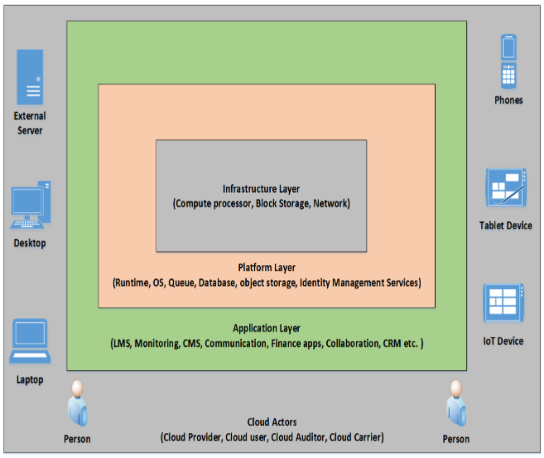

External Server
Desktop
Laptop
Phones
Tablet Device
IoT Device
Infrastructure Layer
(Compute processor, Block Storage, Network)
Platform Layer
(Runtime, OS, Queue, Database, object storage, Identity Management Services)
Application Layer
(LMS, Monitoring, CMS, Communication, Finance apps, Collaboration, CRM etc.)
Person
Cloud Actors
(Cloud Provider, Cloud user, Cloud Auditor, Cloud Carrier)
Person

Figure 2 Cloud Computing Architecture

Various cloud actors like cloud provider, cloud user, cloud auditor & cloud carrier participate in two-way communication with the help of various devices like external server, desktop, laptop, phones, tablet device, IoT device and software APIs. Apart from open stack various other OSS for building cloud setup is also recommended like Eucalyptus, Cloud Stack, Own cloud, Open Nebula etc. [21-25]. It is required to setup some application over the cloud setup like LMS, CRM, CMS etc. On the basis of the experimental setup & the deployed application it will be useful to record the various parameters related to the performance & security. The multilayered architecture is as represented in figure 2. The Process model used for penetration testing & vulnerabilities analysis for experimental setup is as follows:

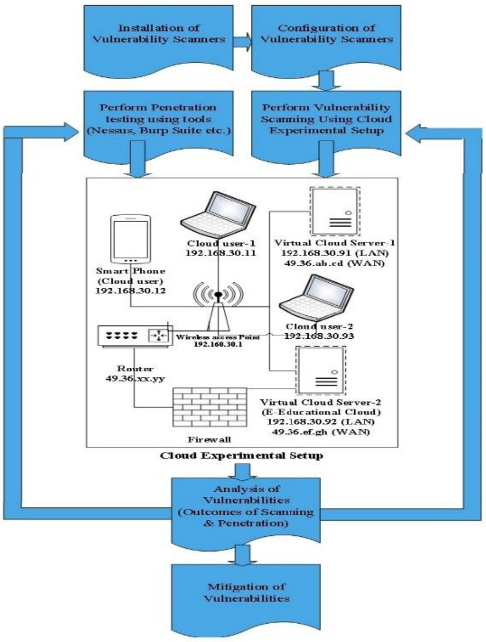

Installation of Vulnerability Scanners
Configuration of Vulnerability Scanners
Perform Penetration testing using tools (Nessus, Burp Suite etc.)
Perform Vulnerability Scanning Using Cloud Experimental Setup
Cloud user-1 192.168.30.11
Virtual Cloud Server-1 192.168.30.91 (LAN) 49.36.ab.cd (WAN)
Smart Phone (Cloud user) 192.168.30.12
Wireless access Point 192.168.30.1
Cloud user-2 192.168.30.93
Router 49.36.xx.yy
Virtual Cloud Server-2 (E-Educational Cloud) 192.168.30.92 (LAN) 49.36.ef.gh (WAN)
Firewall
Cloud Experimental Setup
Analysis of Vulnerabilities (Outcomes of Scanning & Penetration)
Mitigation of Vulnerabilities

Figure 3 Process Model of Vulnerability Scanning & Penetration on Cloud Experimental Setup

Nessus is the most suitable vulnerability scanning tools especially for cloud computing platform. Apart from Nessus following Cloud scanning tools are recommended for performing penetration testing & scanning for vulnerabilities on SPI model:

(i) Nessus (ii) Burp Suite
(iii) Acunetix (iv) IBM Security QRadar
(v) AlienVault USM (vi) InsightVM (Nexpose)
(vii) Intruder (viii) Orca Security
(ix) Detectify (x) Kiuwan
(xi) OpenVAS

4. CLOUD COMPUTING SECURITY ISSUES & CHALLENGES

Before hosting the E-governance application or requirement specific applications over the cloud, it is required to perform investigation of security issues and challenges of the experimental setup. Here the investigation is performed on the basis of SPI model through the reviews. During the investigation of various issues and security challenges are observed and it helps in the formulation of different types of taxonomies related with security issues which further help in analysis of vulnerabilities, threat and attacks [9, 26-30]. Cloud is a superset of technologies, procedures, manpower, and business builds. Like all other technology cloud is also having vulnerabilities. Vulnerability is likelihood that a resource may be incompetent to withstand the movements of a threat agency. While, the discrepancy between the power exerted by threat agent & the entity's capability to withstand that power, vulnerability arises. Cloud Computing (CC) specific vulnerabilities are discussed in table 1 [40-44]

Table 1 CC specific vulnerabilities

Vulnerability	Details
Core Cloud Technology Vulnerabilities	Web applications services, virtualization, and cryptography are all essential cloud computing technologies that have flaws & are either inherent expertise or prevalent in present implementations. There are three examples: (i) Virtual machine escape. (ii) Session hijacking & riding. (iii) Deficient or outdated cryptography.
Cloud Storage misconfiguration	For cybercriminals, cloud storage is a gold mine of stolen data. In spite of high stakes, firms extend to commit fault of misconfiguring distributed storage, which resulted in severe losses for many enterprises. The root reason is misconfigured security groups and a lack of access controls.
Insecure Application Programming Interfaces	To smooth out computational measures, user interfaces are recommended. Regardless, APIs can offer lines of communication for attackers to misuse cloud assets if they are left unprotected. Insecurity in APIs are primarily caused by insufficient authorization and authentication.
IP Loss or Theft	Intellectual property (IP) is certainly very important asset for an enterprise. But at the same time is vulnerable to security threats, particularly if the content is stored over internet. General causes of IP loss or theft include data tampering, data deletion, and loss of access.
Compliance Violations & Regulatory Actions	Cloud provides ease of access, it also create a security risk. The reason behind is the difficulty to control whom are permitted to use cloud data. It is censorious for an enterprise to understand the insights into their information stockpiling & access control to comply with consistency or industry norms.
Loss of Control over End User Activities	When companies don't know in what manner their employees use cloud computing governance, they risk losing control of their data and becoming subject to breaches and insider security threats.

Deficient Management of user Access	The most prevalent security concern is probably improper access management. For numerous years, stolen or lost credentials have been usually employed technique used by attackers in web application or breaches.
Breaches with Clients or business Associates beyond SLA	Cloud SLAs are a little trickier. It typically places restrictions on who has access to information who, where & in what manner it may be used or stored. Employees who transfer critical data in cloud without permission may be in breach of corporate contracts, resulting in legal action.
Defects in Known Security Controls	When cloud innovations directly cause challenges in applying the controls, vulnerabilities in unified security controls must be examine. Control challenges are another term for such vulnerabilities.
Essential Cloud Characteristic Vulnerabilities	The root reasons are unapproved admittance to the administration interface, protocol (IP) vulnerabilities, data recovery vulnerabilities, and metering and billing evasion.
Multi-tenancy Failures	Exploiting system & s/w vulnerabilities in a CSP's assets, computing environment or applications which support multi-tenancy might result in failure of keeping tenants separately. An attacker can take benefit of this failure & gain access to assets or data belonging to another user or organization.
Cloud migration vulnerabilities	When an enterprise thinks through moving its assets/operations among CSPs, vendor lock-in come to be an issue. Due to the following parameters company realizes that the price, effort, schedule time required for the changeover is substantially more from previously estimated: (i) Non-standard data formats. (ii) Non-standard APIs. (iii) Dependency on CSP's proprietary tools. (iv) Uniqueness in APIs.
Compromised CSP supply chain	If CSPs outsource the external agents for their infrastructural operational maintenance than, they may or may not be able to meet the standards that the CSPs have promised to provide to an enterprise. An enterprise must assess how CSP enforces compliance and whether CSPs allows mediators to operate under their own standards. If the parameters are not applied on the supply chain, the threat escalates.

Data privacy and software security are becoming increasingly essential considerations because each type of public, private, or hybrid cloud offers a customizable architecture for streamlined management and cost efficiency. As per CSA, the following are the top threats in a cloud which needs urgent attention are as follows:

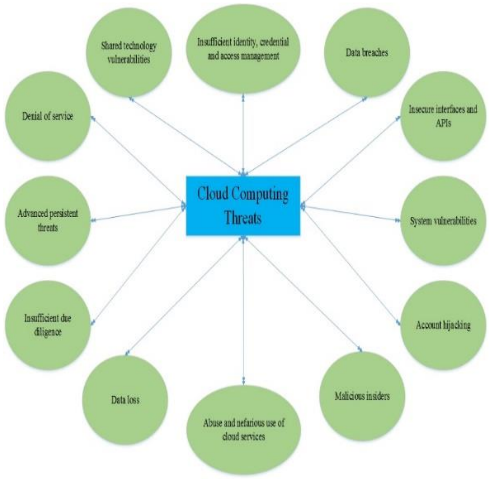

Cloud Computing Threats
Shared technology vulnerabilities
Insufficient identity, credential and access management
Data breaches
Insecure interfaces and APIs
System vulnerabilities
Account hijacking
Malicious insiders
Abuse and nefarious use of cloud services
Data loss
Insufficient due diligence
Advanced persistent threats
Denial of service

Figure 4 Top Cloud Computing Threats

5. RESULTS & DISCUSSION

The investigation of security risk in terms of vulnerabilities are required to be done before deployment of cloud computing based applications. For meeting the business requirement, the IT experts implement respective business process using SPI model. As per NVD / CVE details 18325 vulnerabilities was published in 2020 and 8350 up to first week of June 2021. Apart from them 34740 cloud specific vulnerabilities are published at NIST-NVD till date. The leading CSPs like Google (6034), AWS (112), IBM (5142) also published their vulnerabilities. Based on the SPI model and CVE details (NIST-NVD), the investigation of the security risk in terms of vulnerabilities was performed below as the result:

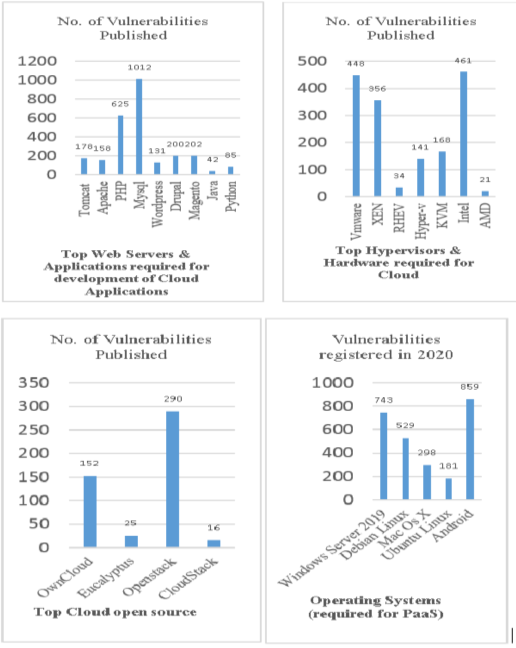
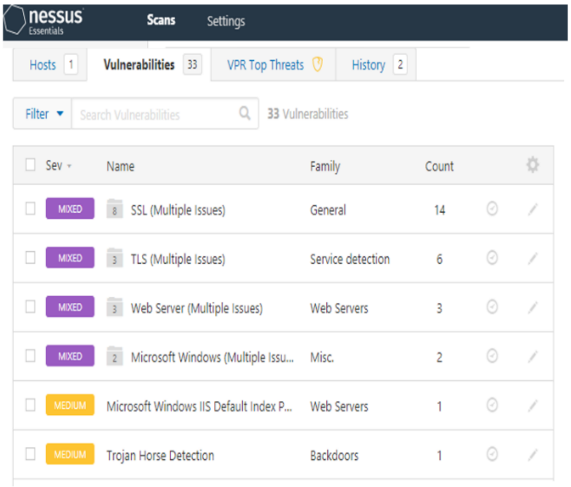


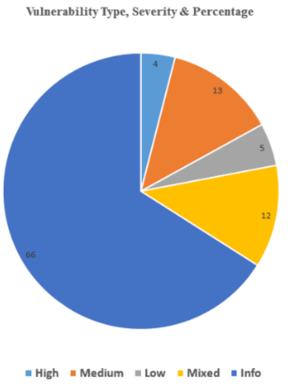
Figure 5 Vulnerabilities based on SPI model

In figure 5a & 5b, the number of vulnerabilities published at NIST-NVD (CVE) of top cloud open source (for IaaS), top hypervisor and Hardware required for building cloud (for PaaS), top web service and applications required for the development of cloud application (for SaaS) and various operating system required (for PaaS) are represented. The real time experiment is performed for investigation of cloud computing security risk in terms of vulnerabilities through deployment of application (LMS for E-educational cloud) on various cloud computing platform and using Nessus as discussed in experimental setup. The results are shown in figure 6:



☐ Sev	Name	Family	Count
☐ MIXED	8 SSL (Multiple Issues)	General	14
☐ MIXED	3 TLS (Multiple Issues)	Service detection	6
☐ MIXED	3 Web Server (Multiple Issues)	Web Servers	3
☐ MIXED	2 Microsoft Windows (Multiple Issu...	Misc.	2
☐ MEDIUM	Microsoft Windows IIS Default Index P...	Web Servers	1
☐ MEDIUM	Trojan Horse Detection	Backdoors	1

(a)



(b)

Figure 6 Vulnerabilities of Cloud application, its type, Severity & Percentage

Findings:

SSL cyphers with medium strength encryption are supported by the remote host. Encryption which use length of key in between 64-112 bits, or which use 3DES encryption suite, is considered medium strength by Nessus. It's worth noting that if the attackers are in the similar physical network as you, it's much easier to get around medium-level encryption. In one or more cypher suites, remote-host enables usage of a block-cypher with blocks of 64bits. As a result, usage of weak 64-bit block cyphers, it is vulnerable to the SWEET32 vulnerability. With appropriate resources, a man-in-the-middle attacker can employ an attack to find a collision & leaks XOR within static secret & identified plaintext, permitting the secret text, like secure https cookies, to be revealed & potentially hijacking an approved session. According to proof-of-concepts, attackers can recover authorization cookies from an http session in 30hrs. It's worth mentioning that this attack requires the client and server to be able to dispatch a huge count of requests on same TLS link. The vulnerability would be mitigated when amount of queries permitted for a distinct connection was reduced. Because Nessus doesn't check this type of mitigation, this plugin requires report paranoia.

To prevent using medium-strength cyphers, reconfigure the affected application. Remove all 64-bit block cyphers from the affected application's configuration. To address this vulnerability, limit the count of requests that can be processed over the same TLS connection.

6. CONCLUSION

For Cloud actors like CSPs & cloud consumers, the cloud computing paradigm is among the supreme promising model for computational services. Form the results it is clear that still investigation of security issues is the most important task and should have first priority. Some of the security issues are due to the technologies that are being used, such as virtualization and SOA. In the paper the investigation of major security issues & challenges related with cloud computing environment are discussed. The cloud specific vulnerabilities are explained with their causes which further provide assistance for identification and analyzing security risk. As a future work the assessment & analysis of risk can be performed using vulnerabilities so as to protect cloud for intruders.

Future Work:

Recognition of a network of diverse objects, threats, and assaults will become increasingly important in the future for confidentiality and protection, and its integration in an IAM framework and supplementary prevention systems is sought & expected. This research will be useful in the future for the creation and implementation of a hybrid strategy that allows for the use of key elements from each of the described methodologies and models. The hybrid design also provides protection and confidentiality safeguards to smart devices in the smart city domain via CC services in the form of a distinct cohesive result. It's also recommended that there's a pressing need to identify the best and most applicable security and confidentiality approaches for certain cloud system in relation of their usability and adoption in the business, particularly in the context of edge, fog, and mobile cloud ecosystems. It is therefore apparent that, in the future, AI and Machine Learning methodologies might be regarded for deep learning of cyber security attacks and threats analysis, such as malware, Trojans, and various attacks, that CC-based Smart city platforms may undergo in order to overcome the substantial threats adversaries this could cause. Furthermore, safety postures must be established to fight and prevent hostile internally and externally exploiters from attacking the CC-based smart city architecture, as well as create repulsive measures against them.

REFERENCES

[1] Mishra N., Singh R.K., Yadav S.K. (2020) Analysis and Vulnerability Assessment of Various Models and Frameworks in Cloud Computing. In: Jain V., Chaudhary G., Taplamacioglu M., Agarwal M. (eds) Advances in Data Sciences, Security and Applications. Lecture Notes in Electrical Engineering, vol 612. Springer, Singapore. https://doi.org/10.1007/978-981-15-0372-6_33

[2] Mamilla, Sushmitha Reddy, "A Study of Penetration Testing Processes and Tools" (2021). Electronic Theses, Projects, and Dissertations. 1220. https://scholarworks.lib.csusb.edu/etd/1220

[3] NIST U.S. Department of Commerce, 2010. NIST Cloud Computing Program – NCCP, https:// www.nist.gov/programs-projects /nist-cloud-computing-program-nccp (accessed March 10, 2018)

[4] Y. Amanatullah, C. Lim, H. P. Ipung and A. Juliandri, "Toward cloud computing reference architecture: Cloud service management perspective," International Conference on ICT for Smart Society, Jakarta, 2013, pp. 1-4, https://doi.org/10.1109/ICTSS.2013.6588059.

[5] Bohn, R. & Messina, John & Liu, Fang & Tong, Jin & Mao, Jian. (2011). NIST Cloud Computing Reference Architecture. 594-596. https://doi.org/10.1109/SERVICES.2011.105.

[6] Kyriakos Kritikos, Kostas Magoutis, Manos Papoutsakis, Sotiris Ioannidis, “A survey on vulnerability assessment tools and databases for cloud-based web applications,” Array, Volumes 3–4, 2019, 100011, ISSN 2590-0056, https://doi.org/10.1016/j.array.2019.100011

[7] I. Yurtseven and S. Bagriyanik, “A Review of Penetration Testing and Vulnerability Assessment in Cloud Environment,” 2020 Turkish National Software Engineering Symposium (UYMS), 2020, pp. 1-6, doi: 10.1109/UYMS50627.2020.9247071.

[8] Omer Bin Tauqeer, Sadeeq Jan, Alaa Omar Khadidos, Adil Omar Khadidos, Fazal Qudus Khan & Sana Khattak, “Analysis of Security Testing Techniques,” Intelligent Automation & Soft Computing, Vol.29, No.1, 2021, pp.291-306, doi:10.32604/iasc.2021.017260

[9] Rakesh Kumar, Rinkaj Goyal, on cloud security requirements, threats, vulnerabilities and countermeasures: A survey, Computer Science Review, Volume 33, 2019, Pages 1-48, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2019.05.002.

[10] J. John and J. Norman, “Major Vulnerabilities and Their Prevention Methods in Cloud Computing,” Advances in Big Data and Cloud Computing, Advances in Intelligent Systems and Computing 750, 2019, https://doi.org/10.1007/978-981-13-1882-5_2

[11] B. R. Mantha and B. G. Soto, “Cyber security challenges and vulnerability assessment in the construction industry”, Proceedings of the Creative Construction Conference 2019.

[12] K. Vijayakumar and C. Arun, “Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC”, Cluster Comput, vol. 22, pp. 10789-

10800, 2019, [online] Available: https://doi.org/10.1007/s10586-017-1176-x.

[13] J. A. D. C. A. Jayakody, A. K. A. Perera and G. L. A. K. N. Perera, "Web-application Security Evaluation as a Service with Cloud Native Environment Support," 2019 International Conference on Advancements in Computing (ICAC), 2019, pp. 357-362, doi: 10.1109/ICAC49085.2019.9103414.

[14] Tahirkheli, A.I.; Shiraz, M.; Hayat, B.; Idrees, M.; Sajid, A.; Ullah, R.; Ayub, N.; Kim, K.-I. A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. Electronics 2021, 10, 1811. https://doi.org/10.3390/electronics10151811

[15] K. A. Torkura, M. I. H. Sukmana, F. Cheng and C. Meinel, "CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure," in IEEE Access, vol. 8, pp. 123044-123060, 2020, doi: 10.1109/ACCESS.2020.3007338.

[16] Ohood M. AlMendah, Dr. Sabah M. Alzahrani, “Cloud and Edge Computing Security Challenges, Demands, Known Threats, and Vulnerabilities,” Academic Journal of Research and Scientific Publishing, Vol 2, Issue 21, 2021, ISSN: 2706-6495

[17] Abhishek Sharma & Dr. Umesh Kumar Singh (2021). Deployment model of e-educational cloud for departmental academics automation using open source. HTL Journal, Volume 27, issue 5, 36, ISSN 1006-6748. https://doi.org/10.37896/HTL27.5/3535

[18] R.Lakshminarayanan, B.Kumar and M.Raju,Cloud Computing Benefits for Educational Institutions, Information Security and ComputerFraud,vol.2,no.1, pp.5-9, 2014.

[19] Ananthi Claral Mary.T, Dr.Arul Leena Rose.P.J., Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art, International Journal of Scientific & Technology Research (2019) Volume 8 Issue 12 ISSN 2277-8616

[20] Mohammed Sadeeq, M., Abdulkareem , N. M. ., Zeebaree , S. R. M. ., Mikaeel Ahmed, D., Saifullah Sami, A., & Zebari, R. (2021). IoT and Cloud Computing Issues, Challenges and Opportunities: A Review. Qubahan Academic Journal, 1(2), 1–7. https://doi.org/10.48161/qaj. v1n2a36

[21] Sefraoui, Omar & Aissaoui, Mohammed & Eleuldj, Mohsine. (2012). OpenStack: Toward an Open-Source Solution for Cloud Computing. International Journal of Computer Applications. 55. 38-42. https://doi.org/10.5120/8738-2991.

[22] Yadav, Sonali. (2013). Comparative Study on Open Source Software for Cloud Computing Platform: Eucalyptus, OpenStack and OpenNebula. Research Inventy :International Journal of Engineering Science. 3. 51.

[23] CloudStack, Accessed on: Dec. 13, 2020. [Online]. Available: https://cloudstack.apache.org/

[24] Open Nebula, Accessed on: Dec. 15, 2020. [Online]. Available: URL: http://opennebula.org/

[25] Shiraz, Muhammad & Abolfazli, Saeid & Sanaei, Zohreh & Gani, Abdullah. (2013). A study on virtual machine deployment for application outsourcing in mobile cloud computing. The Journal of Supercomputing. 63. https://doi.org/10.1007/s11227-012-0846-y.

[26] Tabrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020). https://doi.org/10.1007/ s11227-020-03213-1

[27] Omar Ali, Anup Shrestha, Jeffrey Soar, Samuel Fosso Wamba, Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review, International Journal of Information Management, Volume 43, 2018, Pages 146-158, ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt. 2018.07.009.

[28] Al-Shqeerat, Khalil & Al-Shrouf, Faiz & Hassan, Mohammad & Fajraoui, Hassen. (2017). Cloud Computing Security Challenges in Higher Educational Institutions -A Survey. International Journal of Computer Applications. 161. 975-8887. https://doi.org/10.5120/ijca2017913217.

[29] Ahmed Aliyu, Abdul Hanan Abdullah, Omprakash Kaiwartya, Yue Cao, Mohammed Joda Usman, Sushil Kumar, D. K. Lobiyal & Ram Shringar Raw (2018) Cloud Computing in VANETs: Architecture, Taxonomy, and Challenges, IETE Technical Review, 35:5, 523-547, https://doi.org/10.1080/02564602.2017. 1342572

[30] R. Barona and E. A. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," 2017 International Conference on Circuit, Power and Computing Technologies

(ICCPCT), 2017, pp. 1-8, https://doi.org/10.1109/ICCPCT.2017.8074287

[31] Bhuvaneswary, N., S. Prabu, S. Karthikeyan, R. Kathirvel, and T. Saraswathi. "Low Power Reversible Parallel and Serial Binary Adder/Subtractor." Further Advances in Internet of Things in Biomedical and Cyber Physical Systems (2021): 151.

[32] Bhuvaneswary, N., S. Prabu, K. Tamilselvan, and K. G. Parthiban. "Efficient Implementation of Multiply Accumulate Operation Unit Using an Interlaced Partition Multiplier." Journal of Computational and Theoretical Nanoscience 18, no. 4 (2021): 1321-1326.

[33] Le, Ngoc Tuyen, Jing-Wein Wang, Duc Huy Le, Chih-Chiang Wang, and Tu N. Nguyen. "Fingerprint enhancement based on tensor of wavelet subbands for classification." IEEE Access 8 (2020): 6602-6615.

[34] Naeem, Muhammad Ali, Tu N. Nguyen, Rashid Ali, Korhan Cengiz, Yahui Meng, and Tahir Khurshaid. "Hybrid Cache Management in IoT-based Named Data Networking." IEEE Internet of Things Journal (2021).

[35] Pham, Dung V., Giang L. Nguyen, Tu N. Nguyen, Canh V. Pham, and Anh V. Nguyen. "Multi-topic misinformation blocking with budget constraint on online social networks." IEEE Access 8 (2020): 78879-78889.

[36] Subramani, Prabu, K. Srinivas, R. Sujatha, and B. D. Parameshachari. "Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients." Personal and Ubiquitous Computing (2021): 1-14.

[37] Kumar, M. Keerthi, B. D. Parameshachari, S. Prabu, and Silvia liberata Ullo. "Comparative Analysis to Identify Efficient Technique for Interfacing BCI System." In IOP Conference Series: Materials Science and Engineering, vol. 925, no. 1, p. 012062. IOP Publishing, 2020.

[38] Rajendrakumar, Shiny, and V. K. Parvati. "Automation of irrigation system through embedded computing technology." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 289-293. 2019.

[39] N. Shi, L. Tan, W. Li, X. Qi, K. Yu, "A Blockchain-Empowered AAA Scheme in the Large-Scale HetNet", Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020. 10 .002.

[40] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.

[41] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-empowered Crowdsourcing System for 5G-enabled Smart Cities", Computer Standards & Interfaces, https://doi.org/10.1016/j.csi.2021.103 517

[42] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava and P. Chatterjee, "Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach", IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.3035520.

[43] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang and T. Sato, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," IEEE Transactions on Instrumentation and Measurement, vol. 64, no. 8, pp. 2072-2085, August 2015. https://ieeexplore.ieee.org/document/7138617

[44] K. Yu, L. Lin, M. Alazab, L. Tan, B. Gu, "Deep Learning-Based Traffic Safety Solution for a Mixture of Autonomous and Manual Vehicles in a 5G-Enabled Intelligent Transportation System", IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3042504.