Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

Maximal Security Issues and Threats Protection in Grid and Cloud Computing Environment

Saurabh Gupta
Department of Computer Science, SRM-IST Campus, Ghaziabad
saurabh256837@gmail.com
Sangeeta Rani
Department of Computer Science, SGT University, Gurugram
Sangeeta.sept@gmail.com
Kalpana Batra
Department of Computer Science, SGT University, Gurugram
Kalpana.batra09@gmail.com

----------**ABSTRACT**----------

Cloud computing empowers the sharing of assets for example, storage, network, applications and programming through web. Cloud clients can rent various assets agreeing to their necessities, and pay just for the administrations they use. Be that as it may, in spite of all cloud benefits there are numerous security concerns identified with equipment, virtualization, network, information and specialist organizations that go about as a noteworthy obstruction in the selection of cloud in the IT business. In this paper, we overview the top security concerns identified with cloud computing. For each of these security threats we depict, I) how it very well may be utilized to abuse cloud parts and its impact on cloud elements, for example, suppliers and clients, and ii) the security arrangements that must be taken to forestall these threats. These arrangements incorporate the security procedures from existing writing just as the best security rehearses that must be trailed by cloud heads.

Keywords—**Cloud computing, Data security, Network security**

Date of Submission: Jan 30, 2020 Date of Acceptance: Feb 21, 2020

I. INTRODUCTION

Cloud computing offers numerous favorable circumstances, for example, expanded use of equipment assets, versatility, decreased expenses, also, simple sending. Accordingly, all the significant organizations counting Microsoft, Google and Amazon are utilizing cloud computing. In addition, the quantity of clients moving their information to cloud administrations, for example, iCloud, Google Drive, Dropbox, Facebook and LinkedIn are expanding each day. Numerous business level security arrangements, principles, and practices can't be executed in cloud because of which unique security threats emerge. In spite of the fact that cloud security has been an engaged territory of research in the most recent decade, there are as yet open difficulties in accomplishing it.[1] To control the security hazards in cloud, it is pivotal for analysts, engineers, specialist co-ops, and clients to get them with the goal that they can take most extreme insurances, convey existing security strategies or create new ones. In this paper, the top security threats for cloud computing introduced by Cloud Security Alliance (CSA) have been broke down. The CSA manage presents the security threats for cloud in the request for their seriousness and gives controls that can be trailed by the specialist organizations to maintain a strategic distance from these threats. Be that as it may, these threats and the controls to maintain a strategic distance from them are much referenced explicitly to meet the necessities of industry[2][3]. In this manner, there is a need to study the security threats for cloud and their answers from the exploration viewpoint. In this paper we characterize these threats, portray the manners in which they can be propelled in cloud, the potential approaches to misuse these threats furthermore, their impacts on cloud substances [4]. We have completely investigated and is played the security answers for the anticipation of these threats from writing. Besides, we have characterized these security issues into three classifications which are information security, organize security and cloud condition security (that incorporates issues explicit to cloud condition)[5].

This paper is created as follows: Section II portrays the most basic threats for cloud computing and their belongings on cloud elements. Segment III depicts the security arrangements to dodge these threats, and segment IV gives the finish of paper.

2. THREATS IN CLOUD COMPUTING

In this area the significant threats for cloud computing are investigated. These are:

i) Data threats including information ruptures and information misfortune
ii) Network threats including record or service capturing, and denial of service
iii) Cloud condition explicit threats including uncertain interfaces and APIs, malicious insiders, maltreatment of cloud services, inadequate due tirelessness, and shared innovation vulnerabilities.

Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

2.1 Information threats

Information is viewed as one the most significant important asset of any association and the quantity of clients moving their information to cloud is expanding each day [6]. Information life cycle in cloud involves information creation, travel, execution, capacity and obliteration. Information might be made in customer or server in cloud, moved in cloud through network and put away in cloud stockpiling. At the point when required information is moved to execution condition where it very well may be prepared. Information can be erased by its proprietor to finish its decimation [7].The greatest test in accomplishing cloud computing security is to keep information secure. The significant issues that emerge with the move of information to cloud are that the clients don't have the perceivability of their information and neither do they know its area. They have to rely upon the service supplier to guarantee that the stage is secure, and it executes important security properties to protect their information. The information security properties that must be kept up in cloud are privacy, respectability, approval, accessibility what's more, security [8].Be that as it may, numerous information issues emerge because of ill-advised treatment of information by the cloud supplier. The significant information security threats incorporate information ruptures, information misfortune, unapproved get to, what's more, honesty infringement [9]. These issues happen as often as possible on cloud information. In this paper, we center around information breaks and information misfortune that are portrayed as the two most serious threats to cloud computing by CSA [10].

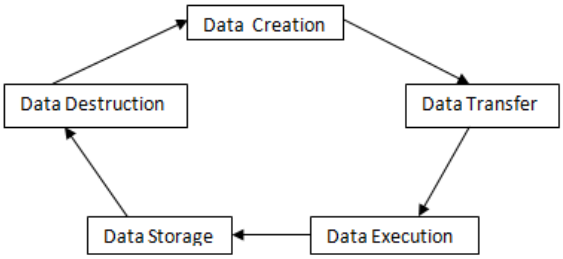
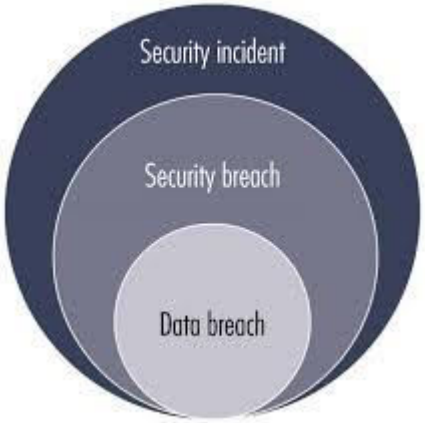


Fig. 1: Data life cycle in cloud computing

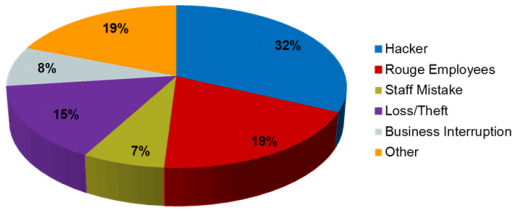
2.2.1 *Data Breaches:*

Data breach is characterized as the leakage of touchy client or association information to unapproved client. Information breach from association can hugy affects its business with respect to back, trust and loss of clients. This may happen accidently because of imperfections in framework, application structuring, operational issues, inadequacy of validation, approval, and review controls [2]. Besides, it can likewise happen because of different reasons, for example, the attacks by malevolent clients who have a virtual machine (VM) on a similar physical framework as the one they need to access in unapproved way. Apple's iCloud clients confronted an information leakage attack as of late in which an endeavor was made to access their private information. Such attacks have likewise been done at different organizations cloud, for example, Microsoft, Yahoo and Google [3][11].



2.2.2 Data Loss:

Data misfortune is the second most significant issue identified with cloud security. Like information breach, information misfortune is a touchy issue for any association and can devastatingly affect its business. Information misfortune generally happens because of vindictive attackers, information erasure, information debasement, loss of information encryption key, blames away framework, or cataclysmic events. 44 percent of cloud specialist organizations have confronted beast power attacks in 2013 that brought about information misfortune and information leakage[2][12]. Additionally, malware attacks have likewise been focused at cloud applications bringing about information annihilation.



3. NETWORK THREATS

Network has a significant impact in choosing how productively the cloud services work and speak with clients. In growing most cloud arrangements, network security isn't considered as a significant factor by certain associations. Not having enough network security makes attacks vectors for the malevolent clients and outcasts bringing about various network threats. Most basic network threats in cloud are account or service hijacking, and disavowal of service attacks [12][13].

3.1 Denial of Service

Denial of Service (DOS) attacks are done to keep the authentic clients from getting to cloud network, stockpiling, information, and different services. DOS

Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

attacks have been on ascend in cloud computing in recent years and 81 percent clients consider it as a critical danger in cloud [1]. They are normally done by trading off a service that can be utilized to devour most cloud assets, for example, calculation power, memory, and network transmission capacity. This causes a postponement in cloud tasks, and here and there cloud can't react to other clients and services. Distributed Denial of Service (DDOS) attack is a type of DOS attacks in which numerous network sources are utilized by the attacker to send an enormous number of solicitations to the cloud for expending its assets [13][14] It tends to be propelled by misusing the vulnerabilities in web server, databases, and applications bringing about inaccessibility of assets.

3.2 Account or Service Hijacking

Account hijacking includes the taking of client certifications to get an entrance to his account, information or other computing services. These taken certifications can be utilized to access and bargain cloud services. [15]

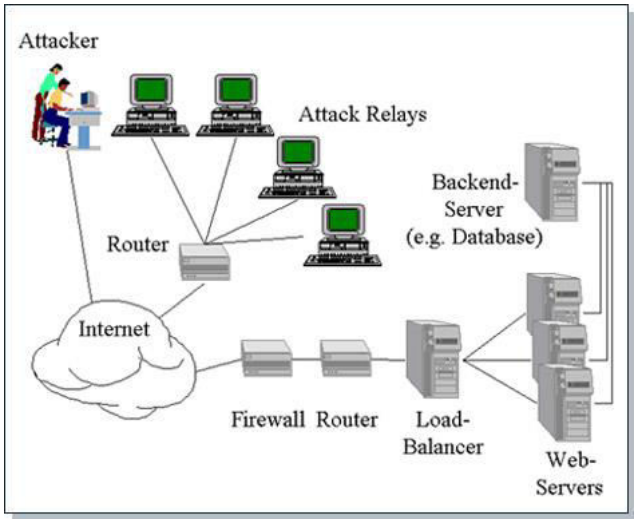
4. CLOUD CONDITION EXPLICIT THREATS

Cloud service suppliers are to a great extent answerable for controlling the cloud condition. In any case, an overview report by Ready Logic shows that right around 50 percent of the cloud clients consider service supplier issues as a significant danger in cloud computing. Aside from service supplier threats, a few threats are explicit to cloud computing, for example, giving uncertain interfaces and APIs to clients, noxious cloud clients, mutual innovation vulnerabilities, abuse of cloud services, what's more, deficient due steadiness by organizations before moving to cloud [16].

4.1 Abuse of Cloud Services

The term maltreatment of cloud services alludes to the abuse of cloud services by the customers. It is for the most part used to depict the activities of cloud clients that are illicit, unscrupulous, or abuse their agreement with the service supplier. Manhandling of cloud services was viewed as the most basic cloud danger in 2010 [2], and various measures were taken to forestall it. Be that as it may, 84 percent of cloud clients still consider it as a pertinent risk [1].

Research has appeared that some cloud suppliers can't recognize attacks propelled from their networks, because of which they can't create alarms or square any attacks. The maltreatment of cloud services is a more genuine danger to the service supplier than service clients. For example, the utilization of cloud network addresses for spam by noxious clients has brought about boycotting of all network addresses; along these lines the service supplier must guarantee all conceivable measures for forestalling these threats. Throughout the years, various attacks have been propelled through cloud by the malevolent clients. For instance, Amazon's EC2 services were utilized as an order and control servers to dispatch Zeus botnet in 2009 [6]. Well known cloud services for example, Twitter, Google and Facebook as an order and control servers for propelling Trojans and botnets. Different attacks that have been propelled utilizing cloud are savage power for secret word splitting of encryption, phishing, performing DOS attack against a web service at explicit host, Cross Site Scripting and SQL infusion attacks.



4.2 Shared Technology Vulnerabilities

Cloud computing offers the provisioning of services by sharing of framework, stage and software. Nonetheless, various segments, for example, CPUs, and GPUs may not offer cloud security necessities for example, impeccable detachment. In addition, a few applications may be planned without utilizing confided in computing rehearses due to which threats of shared innovation emerge that can be abused in numerous manners. As of late, shared innovation vulnerabilities have been utilized by attackers to dispatch attacks on cloud. One such attack is accessing the hypervisor to run noxious code, get unapproved access to the cloud assets, VMs, and clients information. Xen plateform is an open source arrangement used to offer cloud services. Xen hypervisors code makes neighborhood benefit acceleration (in which a client can have privileges of another client) defenselessness that can be dispatch visitor to have VM escape attack[17]

Afterward, Xen refreshed the code base of its hypervisor to fix that weakness. Different organizations, for example, Microsoft, Prophet and SUSE Linux that depended on Xen likewise discharged updates of their software to fix the nearby benefit acceleration weakness. Correspondingly, a report discharged in 2009 [17][18] appeared the use of VMware to run code from visitors to has appearing the potential approaches to dispatch attacks.

4.3 Insecure Interfaces and APIs

Application Programming Interface (API) is a lot of conventions and measures that characterize the correspondence between software applications through web. Cloud APIs are utilized at all the foundation, stage and software service levels to speak with different services. Foundation as a Service (IaaS) APIs are used to get to and oversee framework assets including network and VMs, Platform as a Service (PaaS) APIs give access

Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

to the cloud services, for example, stockpiling and Software as a Service (SaaS) APIs associate software applications with the cloud foundation[19][25].
The security of different cloud services relies upon the APIs security. Powerless arrangement of APIs and interfaces can bring about numerous security issues in cloud. Cloud suppliers by and large offer their APIs to outsider to offer services to clients. In any case, powerless APIs can prompt the outsider approaching security keys and basic data in cloud. With the security keys, the scrambled client information in cloud can be perused bringing about loss of information trustworthiness, secrecy what's more, accessibility [20]. In addition, verification and access control standards can likewise be damaged through shaky APIs.

4.4 Insufficient Due Diligence

The term due perseverance alludes to people or clients having the total data for appraisals of threats partner with a business earlier to utilizing its services. Cloud computing offers energizing chances of boundless computing assets, and quick access due which number of organizations move to cloud without evaluating the threats related with it. Because of the perplexing engineering of cloud, some of association security arrangements can't be applied utilizing cloud. Also, the cloud clients have no clue about the inner security systems, evaluating, logging, information stockpiling, information get to which brings about making obscure hazard profiles in cloud [3].Now and again, the engineers and originators of uses perhaps uninformed of their impacts from sending on cloud that can bring about operational and design issues.

4.5 Malicious Insiders

A vindictive insider is somebody who is a representative in the cloud association, or a colleague with an entrance to cloud network, applications, services, or information, furthermore, abuses his entrance to do unprivileged exercises. Cloud executives are liable for overseeing, administering, and keeping up the total condition. They approach most information and assets, and might wind up utilizing their entrance to release that information [21]. Different classifications of malevolent insiders include specialist programmers who are overseers that need to get unapproved touchy data for no reason in particular, and corporate undercover work that includes taking mystery data of business for corporate purposes that may be supported by national governments.

5. SECURITY TECHNIQUES FOR THREATS PROTECTION

In this section the security strategies to stay away from the abuse of threats referenced in segment II have been discussed. We portray the usage of these security techniques at various levels to verify cloud from threats [22].

5.1 Information Security

5.1.1 Protection from Data Loss

To forestall information misfortune in cloud diverse security measures can be received. One of the most significant measure is keep up reinforcement of all information in cloud which can be gotten to if there should arise an occurrence of information misfortune. Be that as it may, information reinforcement should likewise be ensured to keep up the security properties of information, for example, trustworthiness and privacy. Extraordinary information misfortune counteraction (DLP) components have been proposed in research and scholastics for the counteraction of information misfortune in network, handling, and capacity. Numerous organizations including Symantec, McAfee, and Cisco have likewise created arrangements to execute information misfortune counteraction across capacity frameworks, networks and end focuses. R Chow et al. proposed the utilization of Trusted Computing to give information security. A believed server can screen the capacities performed on information by cloud server and give the complete review report to information proprietor. Along these lines, the information proprietor can be certain that the information get to arrangements have not been abused [11]. Tomoyoshi T. et al. proposed a framework to secure moving information of an organization inside a USB regardless of whether it is lost. They too depict the security of record in its total life cycle also, maintaining a strategic distance from information misfortune through messages [12].

5.1.2 Protection from Data Breaches

Various security measures and techniques have been proposed to maintain a strategic distance from the information breach in cloud. One of these is to scramble nformation before capacity on cloud, and in the network. This will require productive key the executives calculation, and the security of key in cloud. A few estimates that must be taken to maintain a strategic distance from information breaches in cloud are to execute legitimate disengagement among VMs to forestall data leakage, execute legitimate access controls to forestall unapproved get to, and to make a hazard appraisal of the cloud condition to know the capacity of delicate information also, its transmission between different services and networks. Significant measure of research has been completed for the security of information in cloud stockpiling. Cloud Proof [8] is a framework that can be based over existing cloud stockpiles like Amazon S3 and Azure mass to guarantee information respectability furthermore, secrecy utilizing encryption. To verify information in cloud capacity ascribed based encryption can be utilized to scramble information with a particular access control strategy before capacity. In this way, just the clients with get to qualities and keys can get to the information [9]. Another technique to secure information in cloud includes utilizing adaptable and fine grained information get to control [10]. In this plot, get to strategies are characterized dependent on the information

Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

traits. Also, to defeat the computational overhead brought about by fine grained access control, most calculation errands can be given over to entrusted item cloud with unveiling information. This is accomplished by joining techniques of attribute based encryption, intermediary re-encryption, and lethargic re-encryption [23].

5.2 Network Security

5.2.1Protection from Denial of Service

To stay away from DOS attacks it is essential to distinguish and actualize all the fundamental security prerequisites of cloud network, applications, databases, and different services. Applications ought to be tried in the wake of structuring to confirm that they have no provisos that can be abused by the attackers. The DDOS attacks can be forestalled by having extra network data transmission, utilizing IDS that check network demands before arriving at cloud server, and keeping up a reinforcement of IP pools for dire cases. Modern answers for forestall DDOS attacks have additionally been given by various merchants. C. Jin et al. [2][18] proposed a technique named jump check sifting that can be utilized to channel spoofed IP parcels, and aides in diminishing DOS attacks by 90 percent. Another technique for verifying cloud from DDOS includes utilizing interruption location framework in VM [19]. In this plan when an IDS identifies an strange increment in inbound rush hour gridlock, the focused on applications are moved to VMs facilitated on another server farm.

5.2.2Protection from Account or Service Hijacking

Account or on the other hand service hijacking can be maintained a strategic distance from by embracing unique security includes on cloud network. These incorporate utilizing interruption identification frameworks (IDS) in cloud to screen network traffic and hubs for recognizing pernicious exercises. Interruption identification and other network security frameworks must be structured by thinking about the cloud effectiveness, similarity and virtualization based setting [25] [13]. An IDS framework for cloud was structured by joining framework level virtualization and virtual machine screen (liable for overseeing VMs) techniques [14]. In this engineering, the IDSs depend on VMs and the sensor connectors on Snort which is an outstanding IDS [15]. VM status and their remaining task at hand are observed by IDS and they can be begun, halted and recouped whenever by the executive's arrangement of IDS. Character and access the executives ought to likewise be actualized appropriately to stay away from access to certifications. To keep away from account hijacking threats, multifaceted verification for remote get to utilizing at any rate two accreditations can be utilized. A technique that utilizations staggered confirmation at various levels through passwords was made to get to the cloud services. First the client is verified by the cloud get to secret phrase and in the following level the service get to secret key of client is confirmed [16]. In addition, client access to cloud services and applications ought to be affirmed by cloud the board. The reviewing of all the favored exercises of the client alongside data security occasions created from it ought to likewise be done to maintain a strategic distance from these threats [17].

5.3 Cloud Environment Security

5.3.1Protection from Abuse of Cloud Services

The execution of severe beginning enrollment and approval forms can help in recognizing noxious customers. The strategies for the security of significant resources of association should likewise be settled on part of the service level understanding (SLA) between client and service supplier. This will acquaint client about the conceivable lawful activities that can be directed against him in case he disregards the understanding. The Service Level Agreement definition language (SLAng) [21] empowers to give highlights for SLA checking, implementation and approval. Additionally, the network checking should be far reaching for distinguishing malignant bundles and all the refreshed security gadgets in network ought to be introduced.

5.3.2Protection from Insufficient Due Diligence

It is significant for associations to completely comprehend the extent of threats related with cloud before moving their business and basic resources, for example, information to it. The service suppliers must unveil the relevant logs, foundation, for example, firewall to shoppers to take measures for verifying their applications and information [17]. Also, the supplier must arrangement necessities for executing cloud applications, and services utilizing industry gauges. Cloud supplier ought to likewise perform chance evaluation utilizing subjective and quantitative strategies after specific interims to check the capacity, stream, and handling of information.

5.3.3 Protection from Shared Technology Vulnerabilities

In cloud design, hypervisor is answerable for orations of virtual machines and the physical equipment. In this manner, hypervisor must be verified to guarantee appropriate working of other virtualization parts, and actualizing confinement between VMs. Besides, to maintain a strategic distance from shared innovation threats in cloud a technique must be created and executed for all the service models that incorporates framework, stage, software, and client security. The standard prerequisites for all cloud parts must be made, and utilized in structure of cloud engineering. The service supplier ought to likewise screen the vulnerabilities in the cloud condition, and discharge patches to fix those vulnerabilities normally [17].

5.3.4 Protection from Insecure Interfaces and APIs

To shield the cloud from unreliable API threats it is significant for the engineers to structure these APIs by following the standards of confided in computing. Cloud suppliers should likewise guarantee that all the all the APIs executed in cloud are structured safely, also, check

Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

them before sending for potential blemishes. Solid verification instruments and access controls should likewise be actualized to verify information and services from shaky interfaces and APIs. The Open Web Application Security Project (OWASP) [20] gives benchmarks and rules to create secure applications that can help in evading such application threats. Also, it is the duty of clients to examine the interfaces and APIs of cloud supplier previously moving their information to cloud.

5.3.5 Protection from Malicious Insiders

The assurance from these threats can be accomplished by constraining the equipment and foundation get to just to the approved work force. The service supplier must execute solid access control, and isolation of obligations in the administration layer to confine head access to just his approved information and software. Inspecting on the representatives ought to likewise be executed to check for their suspicious conduct. In addition, the representative conduct prerequisites ought to be made piece of legitimate agreement, also, move ought to be made against anybody associated with malevolent exercises [17][26]. To keep information from vindictive insiders encryption can likewise be actualized away, and open networks [27].

6. CONCLUSION

Cloud computing is getting generally embraced in organizations around the globe. Be that as it may, there are distinctive security issues related with it. So as to keep up the trust of clients, security ought to be considered as a basic piece of cloud. In this paper we have concentrated on most extreme threats on cloud computing that are viewed as important by most clients also, organizations. We have partitioned these threats into classes of information threats, networks threats, and cloud condition explicit threats. The effect of these threats on cloud clients and suppliers has been outlined in the paper. In addition, we moreover talk about the security techniques that can be received to maintain a strategic distance from these threats.

References

[1] Jouini, Mouna, and Latifa Ben Arfa Rabai. "A security framework for secure cloud computing environments." Cloud security: Concepts, methodologies, tools, and applications. IGI Global, 2019. 249-263.

[2] George Amalarethinam, D. I., and S. Rajakumari. "A Survey on Security Challenges in Cloud Computing." (2019).

[3] Khan, Nabeel, and Adil Al-Yasiri. "Cloud security threats and techniques to strengthen cloud computing adoption framework." Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. IGI Global, 2018. 268-285.

[4]Zhou, Jun, et al. "Security and privacy for cloud-based IoT: Challenges." IEEE Communications Magazine 55.1 (2017): 26-33.

[5] Hussein, Nidal Hassan, and Ahmed Khalid. "A survey of cloud computing security challenges and solutions." International Journal of Computer Science and Information Security 14.1 (2016): 52.

[6] "Cloud security report spring 2014," https://www.alertlogic.com/resources/cloud-security-report//, last Accessed: 2014-11-08.

[7] "Zeus bot found using amazon's ec2 as c and c server," http://www.theregister.co.uk/2009/12/09/amazon ec2 bot control channel//, last Accessed: 2014-11-15.

[8] "Amazon ec2 cloud service hit by botnet, outage," http://www.cnet.com/uk/news/amazon-ec2-cloud-service-hit-by-botnet-outage/, lastAccessed: 2014-11-15.

[9] K. Kortchinsky, "Cloudburst: A vmware guest to host escape story,"Black Hat USA, 2009.

[10] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang,"Enabling security in cloud storage slas with cloudproof." in USENIX Annual Technical Conference, vol. 242, 2011.

[11] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394,2014.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM, 2010 Proceedings IEEE. Ieee, 2010, pp. 1–9.

[13] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 85–90.

[14] T. Takebayashi, H. Tsuda, T. Hasebe, and R. Masuoka, "Data loss prevention technologies," Fujitsu Scientific and Technical Journal, vol. 46, no. 1, pp. 47–55, 2010.

[15] Roman, Rodrigo, Javier Lopez, and Masahiro Mambo. "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges." Future Generation Computer Systems 78 (2018): 680-698.

[16] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013.

Volume: 11 Issue: 04 Pages: 4367-4373(2020) ISSN: 0975-0290

[17] S. Roche, F. Cheng, and C. Meinel, “Intrusion detection in the cloud,” in Dependable, Autonomic and Secure Computing, 2009. DASC’09. Eighth IEEE International Conference on. IEEE, 2009, pp. 729–734.

[18] “Snort,” https://www.snort.org//, last Accessed: 2015-01-29.

[19] H. Dinesha and V. Agrawal, “Multi-level authentication technique for accessing cloud services,” in Computing, Communication and Applications (ICCCA), 2012 International Conference on. IEEE, 2012, pp. 1–4.

[20] “Cloud controls matrix (ccm), cloud security alliance,” https://cloudsecurityalliance.org/research/ccm/, last Accessed: 2014-12-02.

[21] C. Jin, H. Wang, and K. G. Shin, “Hop-count filtering: an effective defense against spoofed ddos traffic,” in Proceedings of the 10th ACM conference on Computer and communications security. ACM, 2003, pp. 30–41.

[22] A. Bakshi and B. Yogesh, “Securing cloud from ddos attacks using intrusion detection system in virtual machine,” in Communication Software and Networks, 2010. ICCSN’10. Second International Conference on. IEEE, 2010, pp. 260–264.

[23]Angayarkanni, G. "A survey on load balancing in cloud computing using various algorithms." Int J Adv Netw Appl (IJANA) 8.5 (2017): 67-71.

[24] D. Fox, “Open web application security project,” Datenschutz und Datensicherheit-DuD, vol. 30, no. 10, pp. 636–636, 2006.

[25] A. Al Falasi and M. A. Serhani, “A framework for sla-based cloud services verification and composition,” in Innovations in Information Technology (IIT), 2011 International Conference on. IEEE, 2011, pp. 287–292.

[26] Kumar, Sandeep, and Goutam Kumar Saha. "Cloud Computing Security Threats and Attack Detection Issues." International Journal of Applied Research on Information Technology and Computing 10.1 (2019): 38-42.

[27] Gandhi, Vaibhav A., and C. K. Kumbharana. "Comparative study of Amazon EC2 and Microsoft Azure cloud architecture." International Journal of Advanced Networking & Applications (2014): 117-123.

BIBLIOGRAPHY

Saurabh Gupta

I am 31 years old and the brain behind this book. He is a **research scholar** from **Uttrakhand Technical University**, Dehradun. He obtained his **M.Tech** from School of Compute Science & IT, **DAVV**, Indore. He has qualified **CSIR-NET** and **GATE** exam both and having about 6 years teaching experience. Today Saurabh divides his working hours among writing books, teaching classes, conducting training in java/python and making website or portal. He loves to sit in front of his Computer.