International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN(Online): 2350-0557, Volume-10, Issue-3, June 2023
https://doi.org/10.55524/ijirem.2023.10.3.8
Article ID IJIR2386, Pages 44-48
www.ijirem.org

Cloud Security: Challenges and Future Scope

Priyanka Vashisht[1], Shalini Bhaskar Bajaj[2], Aman Jatain[3], and Ashima Narang[4]

[1]Associate Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Gurugram, Haryana, India
[2]Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Gurugram, Haryana, India
[3,4]Assistant Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Priyanka Vashisht; priyanka.vashisht@gmail.com

ABSTRACT- Now Cloud computing becomes so much popular coz satisfying business needs efficiently. Cloud features provide best lead to organizations to effectively access data and services with less cost over the internet. This also raise issues related with cloud security. This paper presents brief information regarding cloud computing security challenges. This information includes security mechanisms that should be consider for Cloud Service Models. This Work also focus on detail knowledge of security issues, threats which may use by attacker. It also explains cloud components levels threats and attack so more secure mechanism can identified for each component. This Paper introduced classification of Cloud security areas issues to develop secure Cloud Security services in future.

KEYWORDS- Cloud Computing, Cloud Security, Threats, Security issues, Data protection, Attacks

I. INTRODUCTION

Cloud Computing provides us various facilities which varies from storing data and access different types of services which are provided by cloud. Also Cloud provide best solutions for business by sharing resources and use readymade infrastructure. This results in reduction of cost and focus on business rather than building infrastructure for business. Resource sharing, data storage, use of cloud application requires very strong security [1].

Basically, Cloud provides us three types of models depending on service they provide to customer. The service models are SaaS, PaaS, and IaaS. SaaS(software-as-a-service) model mainly focuses on access of application provided by Cloud provider. SaaS has risk like access control because of this model one application can be used by many users. example Google provides different software as a service.

Platform-as-a-service (PaaS) model provides development platform for creating various application. Those application data is so valuable so it should be protected from attack. For securing data, encryption is best solution before storing data on data server. Cloud data server should ensure secure data availability for cloud users. Ex. of PaaS Microsoft Azure, Google App Engine. Infrastructure-as-a-service (IaaS) models provides network framework which provides storage for data, standard services. IaaS also provides Virtualization concept. While considering IaaS security we should focus on network security including risks related with firewall, virtual machine. Ex. of IaaS Amazon Web Services (AWS), Microsoft Azure [2].

Cloud also divided into three types according to location of infrastructure. They are public cloud, private cloud, hybrid cloud. Public Cloud is easy to use by end user and it has feature scalability for resources. But it may be not reliable as anyone can access it. Private Cloud provides one framework to organization to run their business. Though Private Cloud is not open to all users but still security of data is major issue as privacy of organization's data is important. Hybrid cloud provides mix services of public cloud and private cloud. Hybrid Cloud security issues includes data protection, application protection, infrastructure protection as visibility is not present [3].

It is so much important to maintain system by security patches. Operating system (OS) and application patches so useful to avoid unauthorized access. In Cloud, consumer should manage system maintenance by installing patches [4]. Cloud provides high performance computing facility, large storage data, capabilities to access different application but most of the business gets affected because of security issues. Cloud Provider and consumer both should have knowledge about IaaS shared responsibility security model. Shared responsibility model recites security duties of both cloud provider and consumer [5]. Next section discussed studied literature of Cloud security.

II. LITERATURE REVIEW

Security policies plays important role to protect data from attacks. Security policies consists of security services for network, data and infrastructure.

A. Security Services

Availability: Availability secures data and service availability to right user on demand. In case of DDos (Distributed Denial of Service) attack it should stop data transfer.

Integrity: Integrity of data provides secure integrity of data should be available to right user. It guarantees data is not change by intruder.

Confidentiality: Confidentiality provides secure data to authorized user. Cloud uses encrypted form of data to make it confidential to store and to transfer. Encryption of data is

useful technique to make it safe from attack.
Authentication: Authentication service related with integrity and confidentiality service with right person. Only those users who have right to access data or service is first identified and then access makes available to that user. SSO (single sign on) is one example of authentication method.
Non-Repudiation: Non-Repudiation service is one type of contract between sender and receiver. Digital signature mechanism is one type of Nonrepudiation service [6].
Sgandurra and Lupu[7] have demonstrate different levels attacks, what attackers wants to achieve. Security should be applied on each level of system it may be OS, application, hardware. They present security issues on each level of system. Kumar et al. [8] have presented various types of data security issues which are applicable for Cloud. Multiuser feature of cloud is a big challenge from security point of view,this is considered by them.Various methods to overcome data security issues are explained in this paper.
Marwane Zekri, et.al[9] explained how intruders uses bugs and vulnerabilities to attack. These bugs and vulnerabilities may present in technology or protocol. The paper also explains DDos (Distributed Denial of service) effect on Cloud service.
MGM Mehedi Hasan et.al [10] demonstrated malicious VM attack also a big challenge in Cloud. The paper explained attacker approach by CAMP game.
Himadri Shekhar Mondal, et.al [11] presents that clouds attacks may get covered but speedy-timely attack detection needed. and explained Fuzzy mechanism for cloud to find out DDoS (Distributed Denial of Service) attack. DDoS attack becomes more problematic if not recognize by security mechanism. Author proposed Fuzzy mechanism which is more secure. Next section explains analysis of studied literature.

III. ANALYSIS OF LITERARURE REVIEW

A. Types of security issues

While considering Cloud Security we should focus on each element of Cloud which plays important role in cloud computing. Following are types of security issues areas.
Storage Data security Issues: In Cloud, data is stored on different server at different location. This distributed storage of network is challenge for security. So it is duty of Cloud Provider to make available Storage data to authenticate user any time. Cloud Provider should be capable of to handle this type of security challenges [12].

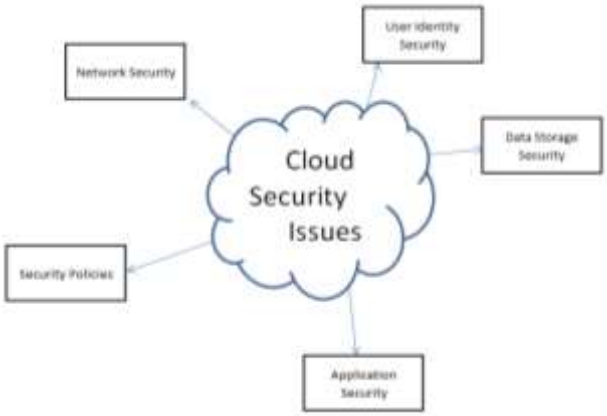

Figure 1: Classification of Cloud security areas

Storage Data security Issues: In Cloud, data is stored on different server at different location. This distributed storage of network is challenge for security. So it is duty of Cloud Provider to make available Storage data to authenticate user any time. Cloud Provider should be capable of to handle this type of security challenges [12].
Application security Issues: Cloud gives ability to access applications to multiusers. The security of these application is big challenge as stealing information ,perform malicious attack on information by attacker done via cloud application.so proper standard secure framework should available to access applications of various platform on cloud [14].
User Identity Security: Cloud provides on demand services including data storage, different resources, application, and network to users. Here managing authorized consumer is challenge. Before providing service checking identity of user is important. Resources can be made available to right user by authorization, authentication, and access management policy. Authentication is process in which user get access of data or resources when user able to present some proof proving he/she is right person to access it. Authentication can be achieved via different techniques. Simple technique of authentication is (credentials)username and password, SSO OTP (One time Password) for accessing multiple services provided by cloud [15].
Authorization is process in which only authorized user who has right to access information or resources can get it. Access levels get assigned to different services of Cloud. Only those users who have that level of access control can use that cloud service. Cloud works with many authorization mechanisms for Security. Mandatory Access Control(MAC) gives possible to achieve confidentiality.MAC provides more secure way to access data and application. Discretionary access control (DAC) determines access permission to each user. Role-based access control (RBAC) Role-based access control allows role access only to authorized users [16].

B. *Security policies Issues*

- Service-level agreement (SLA) is one type of contract between Cloud provider and Cloud consumer.
- SLA mainly focuses on providing and monitoring services. SLA consists of different services and complaints records. SLA describes service performance standard, service response, service availability.
- Cloud business mainly focus on client so client authentication, client access control, access management are important features in cloud security [17].

C. Cloud threat model

Cloud Computing makes business more powerful providing many facilities like resources, infrastructure. Business need to focus purely on business rather than resources. But to maintain and manage cloud security is really big challenge nowadays when an internet user increases rapidly.
Threat model is presentation of vulnerabilities, risks related with system from security point of view. The main aim of threat model is to provide safety and confidentiality to data and resources of cloud. Threat models are organized path to point out and reduce risks. Preeti describes threat model between two VM. Malicious attack can be done by traffic flooding. It can also have done by consuming resources by virtualization [18]. Praerit Garg and Loren Kohnfelder developed Threat model at Microsoft called as STRIDE.

STRIDE mainly divided threats into six categories (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege). Every type of threat has its own type of attacks [19].

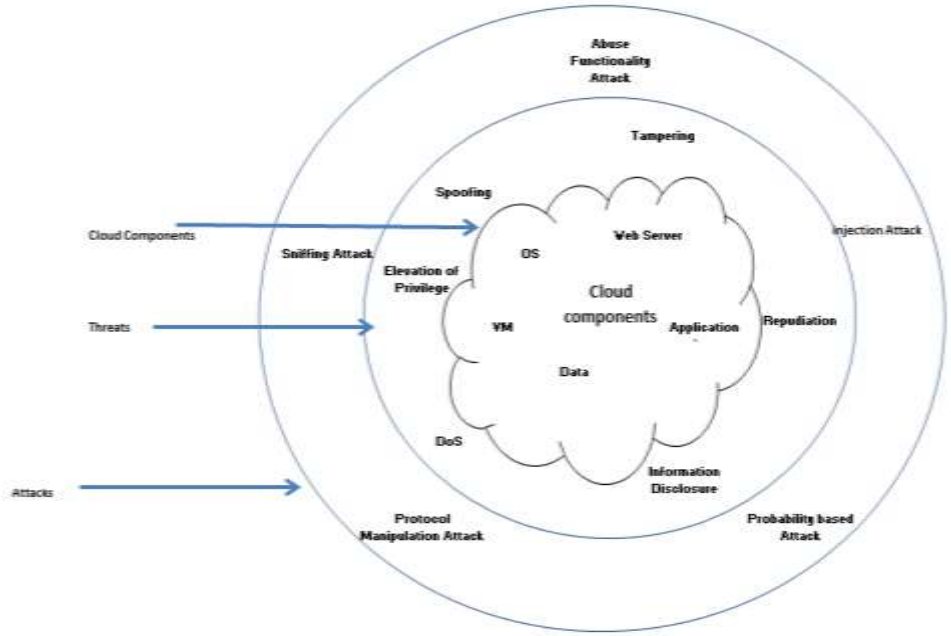

Figure 2: Categories of Cloud components, threats and attacks

Spoofing: Spoofing is act where unacceptable user gains access to communication for stealing someone's personal information. Spoofing done mainly to arrange DoS (Denial of Service) attack which is also achieved through traffic flooding, intrusion links, breaking access control mechanism. IP spoofing and DNS spoofing are main spoofing attacks [20].

Tampering: Tampering is behavior to purposefully destroying or editing data to make it dreadful. By using Tampering one can edit code to break down system. File Integrity Monitoring (FIM) can be useful to find out critical information editing. Cloud computing deals with large amount of data so only confidential critical data can be watched by using cryptography which may be operating system, application, security, and user confidential data. A separate management file system can be maintained for storing log files [21].

Repudiation: Repudiation threat indicates lack of integrity of data. The integrity of data edited, modified by attacker. Availability of origin data service of Cloud gets lost because of Repudiation threat. Cloud security should have security control mechanism to trace user's actions [22].

Information disclosure: Confidential information access by unauthorized user is called as information disclosure. Information disclosure can be done by observing services and their vulnerabilities.VM configuration is also one type of information leakage. Internal type of disclosure can be happened by mistake. But External information disclosure had done for specific purpose by attack. Information disclosure can be avoided by using Encryption, authentication methods [23,24].

Denial of service: DoS (Denial of Service) is an attack made by malicious activities to stop system which results into legal user not accessed services or resources. Distributed Denial of Service (DDoS) attack done after vulnerabilities of network security. This type of attack can be avoided by applying load balancing techniques. Firewall also useful to prevent such network security attacks [25].

Elevation of privilege: Authorization permits access to only privileged level. Elevation of privilege threat is nothing but creation of scenario by attacker that attacker becomes part of trusted system. It becomes dangerous as authentication mechanism avoided by attacker by utilization of vulnerabilities [26].

D. Attacks on Cloud components

A cloud computing model provides lot of facilities, services. Cloud gives ability to use resources available on internet. But while using Cloud, users should be aware of different attacks. Cloud Provider should have enough knowledge regarding Cloud security threats, types of attacks, preventive security measures. Following to OWASP (Open Web Application Security Project) types of attacks we can consider.

Abuse functionality attack: Abuse functionality attack used by attackers to use resources, access control, information leakage to produce unacceptable result. DoS attack, protocol abuse, editing VM configuration are comes under Abuse functionality attack [27].

Injection attack: Injection attack uses unauthorized access to inject changes in code or database. Injection attack leads into different behavior of system. example SQL injection attack [28].

Probability-based attack: Probability-based attacks make full use of delicate cryptography data by different ways. Examples man in middle attack, brute force attack, side channel attacks [29].

Protocol manipulation attack: Protocol manipulation attack comes under network security attacks. Defect in network leads to modification of code, use of communication, denial of services protocol attacks [30].

Resource manipulation attack: Cloud Computing provides availability of data-on-data store. Data storage is one type of resource in Cloud. Resource manipulation attack leads to break down resources which may be files, applications,

information. Example is modification in code [31].
Sniffing attack: Sniffing attacks can gain information from sniffer which is application to catch network traffic. Main target of sniffing attack is to gather network traffic data. Cloud data storage also get affected by sniffing attack [32].

IV. FUTURE CLOUD SECURITY ISSUES

Cloud Computing enables end users to access data, network, resources, infrastructure available on Cloud and concentrate on their work. Nowadays IoTs (Internet of Things) becomes essential part of development. IoTs applications increases rapidly and uses Cloud Computing to store data on cloud storage on anywhere over internet. Cloud Computing provides best solutions for today's world, but this cloud environment also has security risks. It is basic need of Cloud Computing to study threats related with cloud security. Prevention of data, network, resources, infrastructure leads to Secure Cloud. Though many researchers tried to resolve security issues but still increasing use of Cloud Computing facing new security issues like resource sharing, Virtualization, multiuser support which become challenges to researchers.
There is need of Cloud security mechanism which handles all security areas like from cloud computing data to cloud network. Outside attacks can be handled by cloud security mechanism but there should be availability of strong policy for handling inside attacks which are really hard to identify. Efficient Cloud Security framework can be achieved by using latest intelligent technologies.

V. CONCLUSION

Cloud Computing is essential part of business world has ability like scalability, resource availability. Though Powerful opportunities provided by Cloud still some Securities issues present. Here main goal of this paper is to study various security issues, challenges, threat, attacks related with cloud. This study helps to realize various security weaknesses of cloud computing. Presentation of security mechanism, policies provide track for secure Cloud framework.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Subramanian N, Jeyaraj A. (2018). Recent security challenges in cloud computing. Comput Electr Eng 71:28–42. Available: https://doi.org/10.1016/j.compeleceng.2018.06.006

[2] Shi B, Cui L, Li B, Liu X, Hao Z, Shen H. (2018). Shadow monitor: an effective in-VM monitoring framework with hardware-enforced isolation. In: International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, Berlin, pp 670–690. Available: https://doi.org/10.1007/978-3-030-00470-5_31

[3] Bhamare D, Samaka M, Erbad A, Jain R, Gupta L, Chan HA. (2017). Optimal virtual network function placement in multi-cloud service function chaining architecture. Comput Commun 102:1–16. Available: https://doi.org/10.1016/j.comcom.2017.02.011

[4] Deka GC, Das PK. (2018). Application of virtualization technology in IaaS cloud deployment model. In: Design and Use of Virtualization Technology in Cloud Computing: IGI Global, pp 29–99. Available: 10.4018/978-1-5225-2785-5.CH002

[5] Oracle.com. (2018). The Oracle and KPMG Cloud Threat Report 2018 | Oracle (online). Available: https ://www.oracle.com/cloud /cloud -threa t-repor t.html. Accessed 11 Dec 2018

[6] Roman R, Lopez J, Mambo M. (2018). Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst. 78:680–698. Available: https://doi.org/10.1016/j.future.2016.11.009

[7] Sgandurra D, Lupu E. (2016). Evolution of attacks, threat models, and solutions for virtualized systems. ACM Comput Surv. 48(3):1–38. Available: https://doi.org/10.1145/2856126

[8] Kumar PR, Raj PH, Jelciana P. (2018). Exploring data security issues and solutions in cloud computing. Proc Comput Sci. 125:691–697. Available: https://doi.org/10.1016/j.procs.2017.12.089

[9] Marwane Zekri, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. (2017). DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments. 3rd International Conference of Cloud Computing Technologies and Applications. Available: 10.1109/CloudTech.2017.8284731

[10] MGM Mehedi Hasan and Mohammad Ashiqur Rahman. (2017). Protection by Detection: A Signaling Game Approach to Mitigate Co-Resident Attacks in Cloud. IEEE 10th International Conference on Cloud Computing. Available: 10.1109/CLOUD.2017.76

[11] Himadri Shekhar Mondal, Md. Tariq Hasan, Md. Bellal Hossain, Md. Ekhlasur Rahaman and Rabita Hasan, 2017. Enhancing Secure Cloud Computing Environment by Detecting DDoS Attack Using Fuzzy Logic. 3rd International Conference on Electrical Information and Communication Technology (EICT). Available: 10.1109/EICT.2017.8275211.

[12] Mohit P, Biswas G. (2017). Confidentiality and storage of data in cloud environment. In: Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications. Springer, Berlin. pp 289–295. Available: https://doi.org/10.1007/978-981-10-3156-4_29

[13] Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. (2017). DDoS attacks in cloud computing: issues, taxonomy, and future directions. Comput Commun 107:30–48. Available: 10.1016/j.comcom.2017.03.010

[14] Sehgal NK, Bhatt PCP. (2018). Cloud computing concepts and practics. Springer. Available: https://doi.org/10.1007/978-3-319-77839-6

[15] Butun I, Erol-Kantarci M, Kantarci B, Song H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. IEEE Commun Mag. 54(4):47–53. Available: 10.1109/MCOM.2016.7452265.

[16] Zhang Y, Chen X, Li J, Wong DS, Li H, You I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Inf Sci. 379:42–61. Available: https://doi.org/10.1016/j.ins.2016.04.015

[17] Mishra P, Pilli ES, Varadharajan V, Tupakula U. (2017). Intrusion detection techniques in cloud environment:a survey. J Netw Comput Appl. 77:18–47. Available: https://doi.org/10.1016/j.jnca.2016.10.015

[18] Kohnfelder L, Garg P. (1999). The threats to our products. Microsoft Interface, Microsoft Corporation,New York. p 33. Available: Microsoft Defender for Endpoint News and Insights | Microsoft Security Blog

[19] Tounsi W, Rais HJC. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur. 72:212–233. Available: https://doi.org/10.1016/j.cose.2017.09.001

[20] Meinig M, Sukmana MI, Torkura KA, Meinel CJPCS. (2019). Holistic strategy-based threat model for organizations. Proc Comput Sci. 151:100–107. Available: https://doi.org/10.1016/j.procs.2019.04.017
[21] Mokhtar B, Azab MJAEJ. (2015). Survey on security issues in vehicular ad hoc networks. Alex Eng J.54(4):1115–1126. Available: https://doi.org/10.1016/j.aej.2015.07.011
[22] Tan Y, Wu F, Wu Q, Liao XJTJOS. (2019). Resource stealing: a resource multiplexing method for mix workloads in cloud system. J Supercomput. 75(1):33–49. Available: https://doi.org/10.1007/s11227-015-1609-3
[23] Hong JB, Nhlabatsi A, Kim DS, Hussein A, Fetais N, Khan KMJCN. (2019). Systematic identification of threats in the cloud: a survey. Comput Netw. 150:46–69. Available:
[24] Rai S, Sharma K, Dhakal D. (2019). A survey on detection and mitigation of distributed denial-of service attack in named data networking. In: Sarma H, Borah S, Dutta N (eds) Advances in communication, cloud, and big data. Lecture notes in networks and systems, vol 31. Springer, Singapore. Available: http://dx.doi.org/10.1007/978-981-10-8911-4_18
[25] Eldewahi AE, Hassan A, Elbadawi K, Barry BI. (2018). The analysis of MATE attack in SDN based on STRIDE model. In: Proceedings of the International Conference on Emerging Internetworking, Data and Web Technologies, pp 901–910. Available: https://doi.org/10.1007/978-3-319-75928-9_83
[26] Alsmadi I. (2019). Incident response. In: The NICE Cyber Security Framework. pp 331–346. Available: https://doi.org/10.1007/978-3-030-02360-7_13
[27] Wu M, Moon YB. (2017). Taxonomy of cross-domain attacks on cyber manufacturing system. Proc Comput Sci. 114:367–374. Available: https://doi.org/10.1016/j.procs.2017.09.050
[28] Murugan K, Suresh P. (2018). Efficient anomaly intrusion detection using hybrid probabilistic techniques in wireless ad hoc network. Int J Netw Secur. 20(4):730–737. Available: 10.6633/IJNS.201807 20(4).15
[29] Ghose N, Lazos L, Li M. (2018). Secure device bootstrapping without secrets resistant to signal manipulation attacks. In: Proceedings of the IEEE Symposium on Security and Privacy (SP). Pp 819–835. Available: 10.1109/SP.2018.00055
[30] Zhang X, Zhang Y, Mo Q, Xia H, Yang Z, Yang M, Wang X, Lunand L, Duan H. (2018). An empirical study of web resource manipulation in real-world mobile applications. In: Proceedings of the 27th Security Symposium (Security 18). pp 1183–1198. Available: https://dl.acm.org/doi/10.5555/3277203.3277291
[31] Coppolino L, D'Antonio S, Mazzeo G, Romano L. (2017). Cloud security: emerging threats and current solutions. Comput Electr Eng. 59:126–140. Available: https://doi.org/10.1016/j.compeleceng.2016.03.004

ABOUT THE AUTHORS

Dr. Priyanka Vashisht has received her Ph.D from Thapar University, Patiala, M.Tech from Banasthali Vidyapeeth, Rajsthan. She has 20 years of teaching and industry experience. Her areas of expertise include Cloud Computing, Fog Computing and Virtualization. She has authored numerous technical research papers and book chapters in international conferences and journals of repute. She has authored a book. She has 4 patents in her name. She is member of IETE, CSI and ACM.

Dr. Shalini Bhaskar Bajaj completed her Ph.D, from IIT Delhi, M.Tech ,from Delhi College of Engineering, Delhi University. She has more than 20 years of experience in teaching. She has authored numerous technical research papers and book chapters in international conferences and journals of repute. Her research interest are Databases, Data Mining, Predictive Analytics, Pattern Recognition, Cloud Computing. She is Member of IEEE, CSI and IAENG

Dr. Jatain has received her Ph.D from NCU (formely ITM) University, M.Tech from Thapar University, Patiala and B.Tech from M.D U Rohtak. She has more than 14 years of teaching and industry experience. Her research area includes software engineering, Data Mining, Networking, Machine Learning and Optimization techniques. She has authored numerous technical research papers and book chapters in international conferences and journals of repute. She is member of CSI, IETE, IEEE and ACM.

Dr. Ashima Narang has completed her Btech, Mtech and PhD in the field of computer Science from various prestigious institutes of India. Her areas of expertise include Cloud Computing, Security, Software Engineering and Virtualization. She has rich teaching experience of 11 years. She has published numerous research papers in reputed international journals and conferences and has guided students for projects from undergraduate and graduate courses. She is also an active member in the various professional bodies like IAASSE, internet society, SCIEI etc. She is the reviewer to various journals from her expertise field.