IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Cloud Security: Threats, Attacks and Mitigation

K. K. Chauhan[1*], A. K. S. Sanger[2]

[1]Computer Science & Engineering, Meerut Institute of Engineering & Technology, Meerut, India
[2]Computer Science & Engineering, Meerut Institute of Technology, Meerut, India

**Corresponding Author: kamal.chauhan@miet.ac.in*

Available online at: www.ijcseonline.org

Accepted: 18/May/2018, Published: 31/May/2018

Abstract: With tremendous growth of cloud computing in IT industries, cloud security has become one of the major issues that garnered noticeable attention of researchers from industries as well as academia. Cloud computing technology is vulnerable to number of security threats and attacks. Security challenges are major barriers in the adaptation of cloud computing model. Security issues are related to virtualization, network and data including eavesdropping, masquerading, privacy, confidentiality, availability of resources, access control, and identity management. In cloud computing, data are stored on a remote server and accessed through public network. Many of the cryptographic based solutions such as encryption/decryption and digital signature for authentication have been developed. In this paper, we have identified and discussed number of security issues such as authentication, access control, data confidentiality, data integrity, identity management, legal and contractual issues, data breaches, data theft, and unavailability. Moreover, we have also discussed some possible solutions to the security issues and their feasibility and security analysis in real time cloud environment.

Keywords—*Cloud, Data, Security, Threats, Attacks, Mitigation*

I. INTRODUCTION

Cloud computing has become fast growing technology in last few years that increased the capability of IT services without investing in new infrastructure. Due to its benefits like economic, reliability, scalability and quality of service; number of organizations has accepted cloud computing paradigm in their professions. Cloud computing increases the utilization of computing resources making them sharable among number of users. Therefore cloud computing is also called utility computing. Cloud computing provides on-demand Services over Networks (SoN). It allows users to access services or resources anytime and from anywhere in pay-per-use fashion.

Companies such as Google, Amazon, and Microsoft etc. developed cloud infrastructure providing services through Internet. Internet-based services like Gmail and Hotmail are cloud services. Emails are hosted on servers, instead of client's local computer and users can access their email using any device having only a web browser and Internet connection. In last few years, there is huge growth in cloud computing. Many popular web apps such as VoIP (Skype, Google Voice), content distribution (BitTorrent), media services (Picassa, YouTube, Flickr) and other social applications (Facebook, Twitter, LinkedIn) are the examples of world wide acceptance of cloud computing.

The National Institute of Standards and Technology (NIST)[1] defines cloud computing as:"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management efforts or service provider interaction. This cloud model is comprises of five essential characteristics: on-demand self service, broadband network access, resource pooling, rapid elasticity and multi-tenancy; three service models: Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS), and four deployment models: Public cloud, Private cloud, Community cloud and Hybrid cloud.

Numbers of challenges have been encountered in cloud computing models. There are various issues associated with cloud computing [2], [3]. These issues are categorized into various categories varying from security, identity and resource management, energy management, data protection and isolation, availability, heterogeneity and many more. Major challenges that prevent cloud computing from being adopted are: data portability, security, recovery from lost data, cost barrier, performance, and reliability on new technology, virtualization, contractual and legal issues. Cloud computing models are vulnerable to number of security threats and attacks. Security becomes primary concern as services are accessed through Internet. In our study, we identified number of critical and severe security challenges in cloud computing. In this paper, we discussed and analyzed security threats and attacks in cloud computing. Moreover, after analyzing, we also proposed some feasible mitigations techniques to overcome these attacks.

Rest of the paper is organized as follows. Section II describes security threats and attacks in cloud computing. Some ttechniques to mitigate the electiveness of attacks are

discussed in section III. Finally, section IV concludes work in this paper.

II. SECURITY THREATS AND ATTACKS

Security, Performance and Availability are three biggest issues in cloud computing. Due to its characteristics such as multi-tenancy, virtualization, scalability, Internet-based etc, numbers of security threats and attacks are found in cloud service delivery model. The Cloud Security Alliance (CSA) identified following security threats in cloud: Abuse and Nefarious Use of Cloud Computing, Insecure Interfaces and APIs, Malicious Insiders, Shared Technology Issues, Data Loss or Leakage, Account or Service Hijacking and Unknown Risk Profile.

Nature of cloud exposes it to several serious threats such as unauthorized access of data, data theft and intrusions. Key elements in cloud security are found in cloud infrastructure such as in data storage and networks.

.

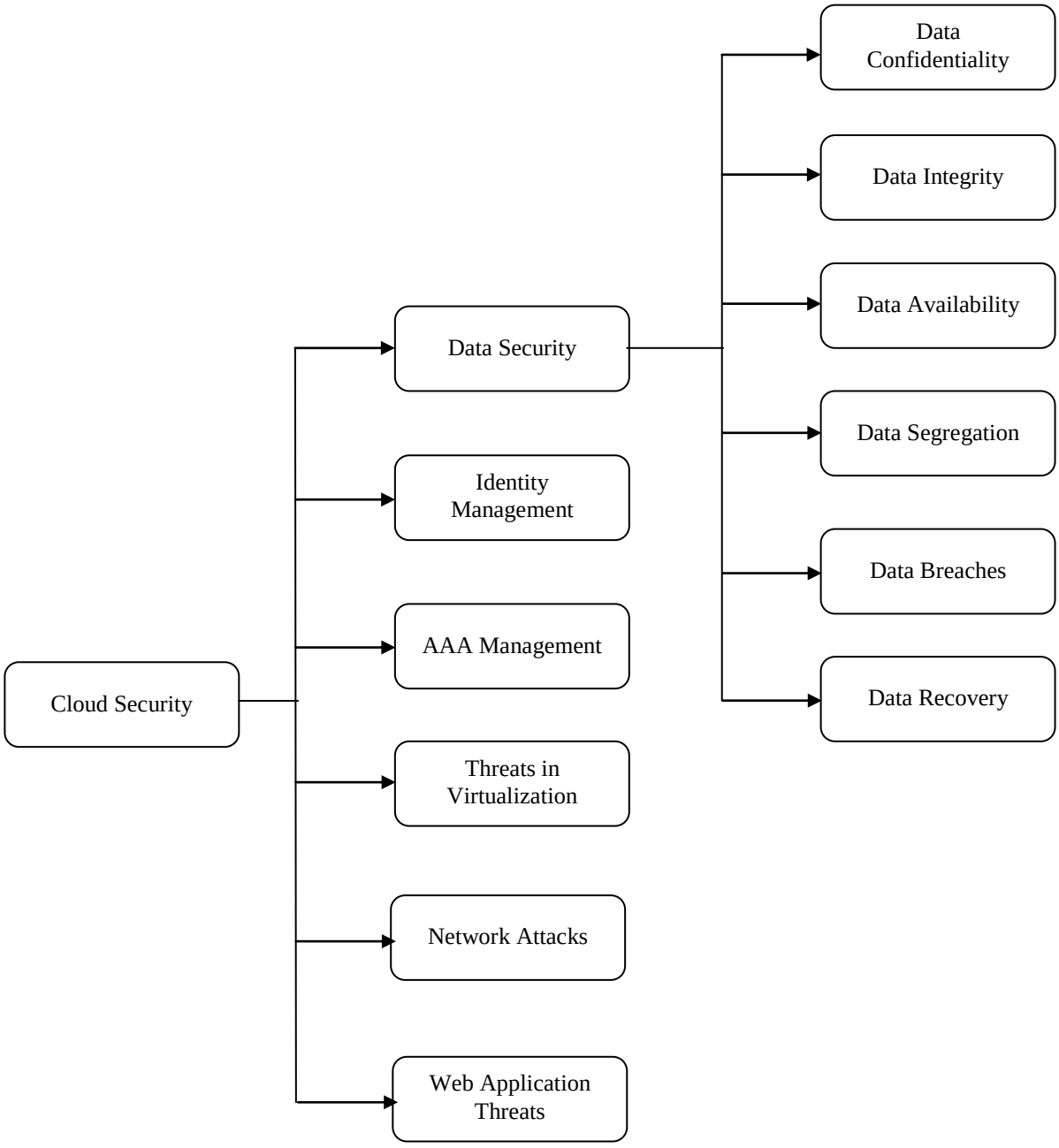

Fig.1: Key Elements in cloud Security

A. Data Security issues:

Data are stores on remote servers; hence data require security in aspect of confidentiality, integrity and availability. Following are the security issues while user storing data on cloud server.

2) Data Integrity: Data Integrity refers to protecting data from unauthorized modification. There must be proper implementation of data integrity on cloud so that data cannot be altered illegitimately.

3) Data Availability: Goal of data availability is to ensure customers that data on cloud can be accessed anytime from anywhere through Internet securely.

4) Data Segregation: Multi-tenancy is one of the characteristics of cloud computing. Data segregation refers to storing data from multiple users on a cloud server. Cloud service providers use multi-tenant infrastructures to maximize cost-effectiveness. There are two issues with multi-tenancy: data separation and geo-location.

5) Data Breaches: Data Breaches is another issue in data security. Various users store large amount of data in the cloud. Hence, there is a possibility that malicious users may also store their infected data or viruses etc. into cloud. This infected data can steal the users' data and send outside and also infect whole cloud server.

6) Data Recovery: There are possibilities of failure of software and hardware or physically damages of hardware due to some accident such as fire or catastrophic. Therefore users can lose their data. Data recoveries become another issue in data security.

B. Identity Management:

Identity Management system manages users' identities with their roles and privileges. Keeping users' identities synchronized with multiple data centers has always been a challenge for an organization. Cloud Service Providers (CSPs) can integrate the users' identity management system into their own infrastructure using federation or single sign on technology or a biometric-based identification system or provide an identity management system of their own.

C. Authentication, Authorization and Accounting (AAA) Management:

Authentication is the process of identifying a user. Generally, a user has to provide some credentials (user name and password) to the system to prove his/her identity. If the credentials match; user is granted permission to access resources. On the other hand, Authorization defines privileges of users to access the system. Not every employee is allowed to access all data. Various access policies have to be implemented to define users' rights and to ensure that data are accessed by authorized users only. Authorization is determined on the basis of attributes of users such as identity and profile. Third, account management refers to the process and standards that keep cloud accounts synchronized with existing enterprise systems.

1) Data Confidentiality: Confidentiality has always been primary requirement; since data are stored on remote server. Data confidentiality ensures the customers that data remain confidential and will not be accessed by any unauthorized user.

D. Threats in Virtualization:

Virtualization technology creates multiple virtual copies of resources of a single instance resource. Number of virtualization technologies includes Storage virtualization, Server virtualization, Operating System-level virtualization, Network virtualization and Application virtualization. Virtual machines increases scalability to the cloud resources. Virtualization provides the features of resource utilization, isolation among hardware, operating system and software. Virtualization allows multi-tenancy to access resources simultaneously on a single physical machine. Following are common threats in virtualization identified by Cloud Security Alliance: VM sprawl, sensitive data within a VM, security of offline & dormant VMs, security of pre-configured VM/active VMs, lack of visibility and control over virtual networks, resource exhaustion, hypervisor security, unauthorized access to hypervisor, account or service hijacking through the self-service portal, workloads of different trust levels located on the same server and Risk due to APIs.

E. Network Attacks:

Cloud computing is an Internet based technology which enables users to access services/resources on network. During data transmission, there are possibilities of data interception and modification. On the other hand, network attacks like eavesdropping, man in the middle attack etc are major challenges. McAfee Labs Threat Report [4] highlights following top seven network attacks in 2016: browser attacks, brute force attacks, Denial of Service (DoS), SSL attacks, port scanning, DNS attacks and backdoor entry.

F. Web Application Threats:

Web threat uses the World Wide Web (WWW) to facilitate cybercrime. It can use different types of malware and fraud that utilize HTTP or HTTPS protocols. Web threats pose a broad range of risks, including identity theft, theft of network resources and loss of confidential information/data etc. Following are most common web threats: SQL injection, cross-site scripting (CSS), session hijacking, buffer overflow, parameter manipulation and DoS.

III. MITIGATIONS

A security model comprises of authentication, access control, availability, confidentiality, integrity and recovery. Numbers of cloud security models are proposed. In this section, we presented some of the security models and their limitations in cloud computing system.

A. Data Security through Encryption and Signing

Encryption based several security models are suggested to secure data in cloud. It is better to encrypt data before moving to cloud. Encryption ensures data confidentiality.

Computing the hash of the data ensures integrity of data. Data integrity check can be provided using RSA Signature.

Wei *et al.* [5] presented a secure protocol SecCloud for data storage security. SecCloud uses encryption for storing data in secure mode. The Merkle hash tree is used for computation security in SecCloud protocol. Table-1 summarizes some proposed schemes for data storage security. Sajithabanu *et al.* [6] proposed a trusted model for cloud computing system. Proposed model consists of backup sites for data recovery. Data is encrypted and compressed during backing up. Hash algorithm is used for the compression. Ruj*et al.* [7] proposed Distributed Access Control in Clouds (DACC) to secure data storage and access. In this model, cloud stores encrypted data in order to secure data storage.

Table-1: Data storage security solution

Proposed Model	Security Services		
	Confidentiality	**Integrity**	**Availability**
Security and privacy for storage and computation in cloud computing[5]	✓	×	✓
Data Storage Security in Cloud[6]	✓	✓	×
DACC: Distributed Access Control in Clouds[7]	✓	×	×
Time-based proxy re-encryption scheme for secure data sharing in a cloud environment [16]	✓	×	×
Security and privacy in cloud computing [20]	✓	✓	✓

Data storage secure schemes proposed above are limited to only when data-in-storage and data-in-transit stage. Encrypted data can be stored on cloud server and exchanged between CSPs and customers' machine. But if data is in processing stage i.e. if a user needs to operate the data. In this case, user needs to decrypt the data then perform operations. Because encrypted data cannot be operated directly. Therefore, traditional encryption methods require decryption of data to be operated. In this way, data is available to cloud provider when data-in-use stage.

Another solution to secure data in data-in-use stage is to apply Homomorphic Encryption (HE) techniques instead of traditional encryption methods. Homomorphic encryption is a kind of encryption that allows users to operate encrypted data. Homomorphic encryption methods are broadly categorized into two categories: Fully Homomorphic Encryption (FHE) and Partial homomorphic encryption. FHE supports unlimited number of operations on encrypted data. On the other hand, partial are limited in aspect of either additive operations or multiplicative operation. First fully homomorphic encryption method is proposed by Craig Gentry in 2009[8]. Former homomorphic encryption techniques are partial. Paillier cryptosystem [9] is a partial homomorphic encryption schemes that support addition operation only. Similarly, RSA cryptosystem support only multiplication operation. Boneh-Goh-Nissim cryptosystem [10] is additive and multiplicative homomorphic encryption that supports unlimited number of addition operations but single multiplication operation. In our study, we found that currently both fully as well as partial are insufficient for cloud data security. Partial HEs are limited to number of operations. Partial HE can be either additive HE or multiplicative HE. RSA cryptosystem is vulnerable to common modulus attack. Suppose C_1 and C_2 are two ciphers encrypted with two RSA public keys (e, n) and (f, n) {gcd (e, f) =1} respectively. If attacker is able to capture C_1 and C_2, he /she can extract M_1 and M_2.

Craig Gentry founder of first FHE also showed that it takes 36 hours to AES evaluate in 2012. However, time is reduced by Homomorphic Encryption library (Helib) [11]. But it did not achieve a feasible time to perform operation on data over Internet.

B. Identity Management and Access Control:

Identity Management and access Control (IDMC) mechanism defines the roles and privileges of users on cloud system. Dhungana*et al.* [12] presented an identity management framework for cloud infrastructure. The authorization manager handles the service requesting and service management. Proposed solution ensures the users' identity and access control. Guojun Wang *et al.* [13] proposed a Hierarchical Attribute-Based Encryption for access control in cloud computing. This model combines the hierarchical identity-based encryption (HIBE) system and the cipher text-policy attribute-based encryption (CP-ABE) system. Z. Wan *et al.* [14] is a Hierarchical attribute-based solution (HASBE) for access control and privacy protection through encryption in cloud computing environment; HASBE is driven from Cipher text Policy attribute-based encryption (CP-ABE) with a hierarchical structure of cloud users. Proposed approach achieves scalability, flexibility and access control of data in cloud. Table-2 illustrated some of the identity management and access control schemes.

Table-2: Identity management and access control solution

Proposed Scheme	Security Services	
	Identity Management	Access control
Identity management framework for cloud networking infrastructure [12]	✓	✓
Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services (HABE) [13]	×	✓
Hierarchical attribute-based solution for flexible and scalable access control in cloud computing (HASBE) [14]	×	✓
Identity-based encryption from the Weil pairing [15]	×	✓

C. Contractual and legal Issue:

Contractual issues like initial due diligence, contract negotiation, implementation, termination, supplier transfer must be considered in cloud computing. The solutions to contractual and legal scheme are proposed in [12], [17]. Rak*et al.* [17] proposed a SPECS method that ensures SLA-based security. The proposed architecture focused three aspects: negotiation, enforcement, and monitoring. M.L. Hale and R. Gamble [18] proposed secure agreement protocol Secagreement to minimize risk service among levels of service to fulfil the users need.

Table-3: Contractual and legal Issue solutions

Proposed Scheme	Monitoring	Negotiation
Security as a service using an SLA-based approach via SPECS [17]	✓	✓
Secagreement: advancing security risk calculations in cloud services [18]	×	✓

D. Securing Virtualization:

CSP must ensure data security; when it embarks on a server virtualization. Security risks in virtual environment can be broadly classified into three types [19].

1) Architectural: The layer of abstraction lies between physical hardware and virtualized systems. A VM can be target of attacks from other VMs on same network.

2) Hypervisor software: A hypervisor or virtual machine monitor (VMM) is software that creates and runs virtual machines. Security vulnerability in the hypervisor is software/tools.

3) Configuration: Configuring new infrastructure and rapidly deploying virtual system becomes critical task.

Cloud provider must identify and resolve these security risks and controls to address them before providing services to users. Service provider should provide guide lines for technical characteristics of the virtualization, including security services and cryptographic mechanisms to protect data communications. Most of the implementation includes selection of virtualization software, storage system, and network topology and bandwidth availability. There must be authentication system for the application/server, guest operating system and hypervisor to provide different layers of security and protection. Proper encryption/decryption is required to significantly reduce the risk associated storage containing users' sensitive data. Together with periodic audits of the virtualized environment will help to identify and mitigate challenges and vulnerabilities. Cloud Security Alliance (CSA) identified eleven major risks in virtual environment. Detail discussion on security impact of these risks and security control for mitigate is beyond the paper. Therefore, we didn't discuss in detail.

IV. CONCLUSION

Cloud computing provide on demand computing resources or services to customers through Internet with minimal effort. Open access to public network leads to many security threats. In this study, we highlighted security issues and proposed some possible security models in cloud computing system. Several security issues, vulnerability and attacks in cloud environment related to data storage, network attacks, web application issues, legal issues, virtualization etc. are discussed. Cryptographic based solutions have been proposed by many researchers. To provide a secure and adaptable cloud environment, encryption techniques can be used for storing and retrieving data from cloud. Hashing methods are used to ensure integrity of users' data. Key management techniques to manage cryptographic keys must be used to distribute the keys to the cloud users. In the final section, we addressed possible solutions for the security issues that provide secure cloud environment. During the study, we also found conventional encryption techniques are not sufficient to secure data in transit state. Hence, there is requirement homomorphic encryption in cloud computing. Finally, we analyzed several security issues in order to realize implementation of cloud computing and number of security solutions including identity management, contractual and legal issue for different types of cloud services; which makes it simple, feasible and reliable technology.

REFERNCES

[1]. P. Mell, T. Grance, "NIST Definition of Cloud Computing", 2011.

[2]. "Top Threats to cloud Computing", Cloud Security Alliance (CSA), 2010.

[3]. Y. Ghanam, J. Ferreira, F. Maurer, "Emerging issues & challenges in Cloud- A hybrid approach". Journal of software engineering and applications, vol. 5, no. 11, pp.923-937, 2012.

[4]. McAfee Labs Threats Reports, 2016.

[5]. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, "Security and privacy for storage and computation in cloud computing", ACM International Journal of Information Science, vol. 258, pp.371–386, 2014.

[6]. S. Sajithabanu, E. G. P. Raj, "Data Storage Security in Cloud". International Journal of Computer Science and Technology, vol. 2, no. 4, pp.37-44, 2011.

[7]. S. Ruj, A. Nayak, V. Stojmenovic, "DACC: Distributed Access Control in Clouds". In the proceeding of International Joint Conference of IEEE TrustCom, pp.91-98, 2011.

[8]. C. Gentry, "A Fully Homomorphic Encryption Scheme", 2009.

[9]. P. Paillier, "Public-key Cryptosystems based on Composite Degree Residuosity Classes". In the proceeding of International Conference on Theory and Application of Cryptographic Techniques, Heidelberg: Springer-Verlag, pp.223–238, 1999.

[10]. R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems". Communications of the ACM, vol. 2, pp.120–12, 1978.

[11]. S. Halevi and V. Shoup, "Design and Implementation of a Homomorphic - Encryption Library", Nov, 2012.

[12]. R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, "Identity management framework for cloud networking infrastructure". In the proceeding of IEEE International Conference on Innovations in Information Technology, South Africa, pp.13–17, 2013.

[13]. G. Wang, Q. Liu, J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", In the proceeding of 17thACM conference on Computer and communications Security, USA, pp.735-737, 2010.

[14]. Z. Wan, J. Liu, R.H. Deng, "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing". IEEE Transaction Information Forensics Section, vol. 7, no. 2, pp.743–754, 2012.

[15]. Boneh, Dan, M. Franklin, "Identity-based encryption from the Weil pairing", SIAM Journal on Computing", vol. 32, no.3, pp.586-615, 2003.

[16]. Q. Liu, G. Wang, J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment", ACM International Journal Information Science, vol. 258, pp.355–370, 2014.

[17]. M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, "Security as a service using an SLA-based approach via SPEC".In the proceeding of 5th IEEE International Conference on Cloud Computing Technology and Science, UK, pp.1-6, 2013.

[18]. M.L. Hale, R. Gamble, "Secagreement: advancing security risk calculations in cloud services". In the proceeding of 8th IEEE World Congress on Services, pp.133-140, 2012.

[19]. "Best Practice for Mitigating Risks in Virtual Environments", Cloud Security Alliance (CSA), April, 2015.

[20]. Z. Tari, "Security and privacy in cloud computing". IEEE Cloud Computing, vol. 1, no. 1, pp.54–57, 2014.

[21]. A. Singh, K. Chatterjee, "Cloud security issues and challenges: a survey". Elsevier Journal of Network and Computer Application, vol. 79, no. 1, pp.88-115, 2016.

[22]. K. K. Chauhan, A. Sanger, A. Verma, "Homomorphic Encryption for Data Security in Cloud Computing", In the proceeding of 14th IEEE International conference on Information Technology, India, pp.206-209, 2015.

[23]. S. Subashini, V. Kavitha, "A Survey on Security issues in Service delivery models of Cloud Computing", Elsevier Journal of Network and Computer Applications, vol. 34, pp.1-11, 2011.

[24]. N. Jain, P. Sharma, "A Security Key Management Model for Cloud Environment", International Journal of Scientific Research in Computer Science and Engineering, vol.5, issue.1, pp.45-48, Feb-2017.

[25]. S. Kathuria, "A Survey on Security Provided by Multi-Cloud in Cloud Computing", International Journal of Scientific Research in Network Security and Communication, vol.6, issue.1, pp.23-27, Feb-2018.

[26]. M.A. Khan, "A Survey of Security issues for Cloud Computing", Elsevier Journal of Network and Computer Applications, vol. 71, pp. 11-29, 2016.

Authors Profile

Mr. Kamal Kumar Chauhan pursued Bachelor of Technology from UP Technical University, Lucknow, India in 2008 and Master of Technology from ABV-Indian Institute of Information Technology &Management, Gwalior in 2010. Currently, he is working as Assistant Professor in Department of Computer Science &Engineering, Meerut Institute of Engineering &Technology, Meerut, India. He has 8 years of experience of academics. He has published number of research paper in international conference including IEEE/Springer and international journals. His main areas of researches are Cryptography, Network Security, Cloud Security & Privacy and Ad Hoc Networks.

Mr. Amit Kumar Singh Sanger pursued Bachelor of Technology from UP Technical University, Lucknow, India in 2005 and Master of Technology from ABV-Indian Institute of Information Technology & Management, Gwalior in 2010. Currently, he is working as Assistant Professor in Department of Computer Science &Engineering, Meerut Institute of Technology, Meerut, India. He has more than 10 years of experience of academics and 1 year experience of software development. He has published number of research paper in conference including IEEE/Springer and international journals. His main areas of research are Computer Architecture, Cloud Computing, Genetic Algorithms and Neural Networks.

