A Review of Cloud Computing Environment and Security Challenges

Dr. Savita, Satish Kumar

***Abstract*—Cloud computing exhibits a remarkable potential to offer cost-effective and more flexible services on-demand to the customers over the network. It dynamically increases the capabilities of the organization without training new people, investment in new infrastructure or licensing new software. Cloud computing has grown dramatically in the last few years due to the scalability of resources and appear as a fast-growing segment of the IT industry. The dynamic and scalable nature of cloud computing creates security challenges in their management by examining policy failure or malicious activity. In this paper, we examine the detailed design of cloud computing architecture in which deployment models, service models, cloud components, and cloud security are explored. Furthermore, this study identifies the security challenges in cloud computing during the transfer of data into the cloud and provides a viable solution to address the potential threats. The task of Trusted Third Party (TTP) is introducing that ensure the sufficient security characteristics in the cloud computing. The security solution using the cryptography is specifically as the Public Key Infrastructure (PKI) that operates with Single-Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) which ensure the integrity, confidentiality, availability, and authenticity involved in communications and data.**

Keywords—Cloud computing; deployment models; service models; cloud security; trusted third party; cryptography

I. INTRODUCTION

Cloud computing extends the information technology capabilities by increasing the capacity and adds abilities dynamically without investing on large and expensive infrastructure, licensing software, or training new personals. Among the several benefits, cloud computing provides a more flexible way to access the storage and computation resources on demand. In the last few years, different business companies increasingly understand that by tapping the cloud resources and gaining fast access, they are able to reduce their initial business cost by paying only the resources they used rather than the need of potentially large investment (owning and maintenance) on infrastructure. [1]-[3]. Cloud computing is explained by National Institute of Standard and Technology (NIST). It is a model to enable convenient, ubiquitous and on-demand network access that is the configurable computing resources to shared resources which can be delivered and provisioned rapidly with minimum managerial interaction [4].

The cloud is the collection of virtualized and inter-connected computers that consists of parallel and distributed systems which can be dynamically presented and provisioned the computing resources based on some Service Level Agreements (SLA) that is established by the settlement between the customers and service provider [5]. Many companies like Microsoft, Google, Amazon, IBM, etc. developed the cloud computing systems and provide a large amount of customers by enhancing their services [6]. Moreover, there are significant barriers to adopting cloud computing like security issue regarding the privacy, compliance and legal matters because it is relatively new computing model having a great deal of the uncertainty regarding the security of all levels such as host, network, data levels, and application can be accomplished [7]. The increment in the adoption of cloud computing and the market maturity is growing steadily because the service providers ensure the complex security level, compliance and regulatory. In part this growth, the cloud services will deliver the increased flexibility and cost savings [10].

This research explains the overview of cloud computing architecture as: 1) cloud deployment models; 2) cloud service model; 3) cloud basic characteristics; 4) cloud security. Security concerns of different companies with the growing importance of cloud resources are taking into account when the data migrate to the modernize cloud systems, advances in business needs and the impact of services offered by the different organizations to increase the market. The suggested solution to the horizontal level services which are available for the concerned entities that basically maintain trust to realize the security mesh. Public Key Infrastructure (PKI) operates with Single-Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) and is utilized to securely

authenticate and identify the concerned entities.

II. CLOUD COMPUTING ARCHITECTURE

NIST is responsible for providing security in the cloud computing environment and developing standards and guidelines which shows a valuable contribution that offers a better understanding of cloud services and computing technologies [2], [12]. Cloud computing architecture summarize as the four deployment models: public cloud, private cloud, community cloud, and the hybrid cloud. The deployment models represent the way that the computing infrastructure delivers the cloud services can be employed. The three cloud service models or delivery models are available for the customer: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are different levels of security required for these service models in the cloud environment. The wide range of services considered in cloud basic characteristic layer that can be used all over the internet. The cloud security is the very important and complex task when the data transfer or shared resources to the cloud within the client-server architecture. The architecture of cloud computing is shown in Fig. 1 and details are discussed as follows:

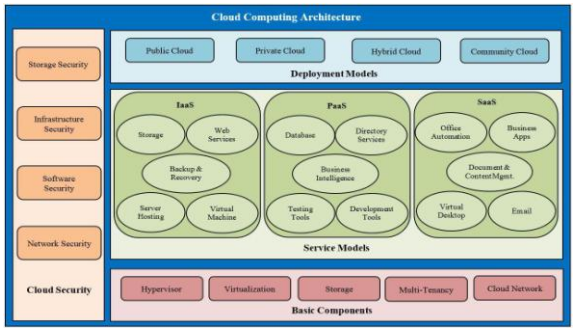

Fig 1: Cloud Computing Models

The cloud computing model has three deployment models that can be particularly used to represent the cloud service models and it explains the nature and purpose of the cloud. The deployment models can be shown in Fig. 2 and classified as follows:

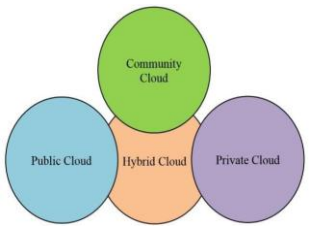

Fig. 2.Cloud deployment models.

1) Public Cloud: A public cloud represents the cloud hosting and owned by the service provider whereby the client and resource provider have service level agreement [4], [13]. Microsoft, Google, Amazon, VMware, IBM, Sun and Rack space are some examples of cloud service provider. The platform is designed in the form of generalized computing that holds the generic type of customer demand. It contains some concerns over privacy, data access and security for customers because it is outside the firewall. It is less secure than the other deployment models and suited for a small and medium business that may not have to configure servers and purchase capital resources.

2) Private Cloud: The cloud infrastructure is managed and maintained by the single organization that compromises multiple customers. If any organization set up their own private cloud and recently create their own servers having physical hardware servers that put virtualization layer top on them then they would make resources available only internally. So, their application can deploy to their own physical control server, they don't need to go Microsoft or Amazon servers. They will set up their own infrastructure. It can ensure the physical security and more secure as compared to the public cloud because of its specific internal exposure. Private cloud is the only access to operate by the designated stakeholder and organization.

3) Hybrid Cloud: Hybrid cloud is referred as the combination of two or more cloud deployment models that can be either public, private or community clouds which remain the unique entities but are bound together [15]. The importance of hybrid cloud usually offers extra resources when the high demand from the customer and for instance it is enabled to migrate some computation jobs from private to public cloud. It is well organized and allows different entities to access data over the internet because it offers more secure control of the applications and data. Hybrid cloud gets more popularity and became a dominant model. The main reason is that it has the ability to take advantage of cost-saving, scalability in elasticity that public cloud may provide, allow control flexibility when it needed.

4) Community Cloud: Community cloud is referred as

the organizations shared its cloud infrastructure among the customers having similar interest or concerns like a policy, the security requirements, and mission and compliance consideration. We say that the several organizations or a third party are operated, controlled, shared and handled the resources of community cloud [16]. In case of the third party like Siemens have IT services and solutions that set up a media cloud for the media industry.

III. Cloud Security

Cloud security is the set of control-based policies, compliance and technologies designed to deploy the protection of applications, data and infrastructure associated with the cloud. Cloud is used by more organizations and associated providers for operating data have become the priority to contract for proper security and potentially vulnerable areas. Cloud computing security is the major concerns when shared resources, access control, privacy and identity management needs [32]. Some of the concerns are discussed as follows:

- The data store in the cloud can be deliberately disclosed by the cloud providers, employees and its contractors.
- Cloud-based data may be incorrectly modified and vulnerable to delete (lost accidentally) by the service provider.
- In the public network, the data may be possibly accessible through the insecure APIs and protocols.
- The resources in the cloud are typically shared with different tenants that may be attacked.

Although, the security of data is in-fact challenging when data transfer to the cloud. This section briefly discusses the security concerns as follows:

1) *Cloud Storage Security*: The popularity and adoption of cloud storage is rising that produce many security challenges for the cloud providers as well as for the customers. IT experts to warn that every kind of technologies even virtual or physical, it contains inherent risks when using file-sharing applications and cloud storage. Customers store their data in the cloud have no longer owns the data because it will transfer through the third party that means the privacy setting of data is beyond the control of service provider or enterprises [33]. Customers need to ensure the quality of service and security of the data in the cloud. The security concerns about storage are data leakage, BYOD (Bring Your Own Data), snooping, cloud credentials and key management.

2) Cloud Infrastructure Security: Cloud computing enabling the distributed workforce and provides many benefits for the customers but it is essential to learn how to operate the cloud infrastructure that ensures and verify the secure deployment of services, storage of data, communication and safe operation through administration [21]. With the rapid adoption of cloud services, the concerns (privacy, security and reliability) have emerged as potential barriers. Information security professionals usually define the security guideline, rules and practice of cloud infrastructure of the organization at the application, host and network levels.

3) Software Security: The cloud provider required to protect their applications or software from internal and external thread throughout from design to production in their entire life cycle [34]. It is important to define the security process and policies about the software that enables the business instead of introducing other risk and it poses challenges for the customers and the cloud provider. Software security can be handled or defeat by implementing bugs, design flaws, buffer overflow, error handling agreements.

4) Cloud Network Security: A cloud service provider has the responsibility to allow the only valid network traffic and block all malicious traffic. Cloud providers are not shared the internal network infrastructure like the access routers and switches employ to connect cloud VMs to the provider network. The customer concerned on internal network attacks which include 1) leakage of confidential data; 2) unauthorized modification; and 3) denial of service or availability. Network security has concerns from both internal and external attacks because the attacker may legally authorize from another part of the network and attack can occur either physical or virtual network [34].

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

The applications of cloud services are operating in the cloud computing infrastructures by using the internet or internal network. The concept of trust in the organization can be referred as the customers assure the capabilities of the organization that it provides the required services reliably and accurately. Trust in cloud computing environment based on the selected cloud deployment models in which the applications are delegated and outsourced to the control of the owner. Trust has required an efficient and effective security policy in the traditional architecture that addressed the functional constraints and flows between them [35], [36]. It is believed that transfer of data or any association of organization or systems to the outside organization that opening a way to gain unauthorized access to the information resources [37].

These major security aspects are required to secure the data, hardware and software resources. Furthermore, discusses the Trusted Third Party (TTP) in the cloud computing environment through enabling trust and cryptography [38]. The cryptography is used to ensure the authenticity, confidentiality and integrity of data by trying to address the specific security vulnerabilities. Third parties or Cloud providers exhibit the trust of customers with specific quality, operational and ethical characteristics, and it comprises the minimal risk factor acknowledgment. TTP in the IS which is offering scalable end-to-end security services that depend on the standards and suitable in separate administrative domains, specialization sectors, and geographical areas. The security challenges of cloud computing infrastructure that can be considered in detail as follows:

A. Integrity

Data integrity in cloud computing is the preservation of data that is stored in cloud server to verify the data is not modified or lost by employing the services of the third party. Organizations can achieve more confidence to prevent system and data integrity from unauthorized access [39].

The data integrity involves the three main entities: 1) a cloud storage provider to whom outsourced the data; 2) owner of data outsource his data; and 3) auditor who ensures the data integrity. The auditor may be the owner of data or he can assign responsibility to a third party [40]. The process of data integrity scheme defined as in two phases and is shown in Fig. 4. The pre-processing phase includes the pre-processed data and generated some additional metadata. The verification of proof done by the auditor that ensures the data integrity is intact.

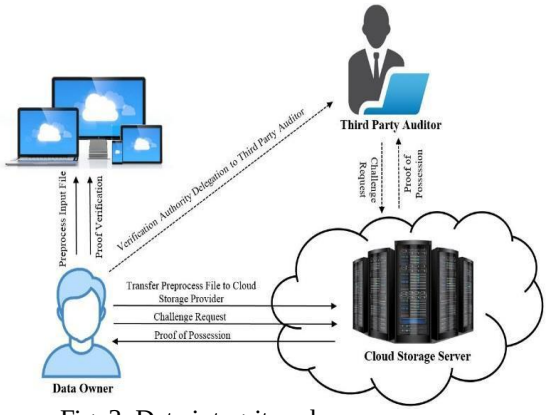

Fig. 3. Data integrity scheme.

The timely identification of any data deletion or corruption by using the data integrity scheme and takes necessary measures for the recovery of data. The data integrity scheme contains some design challenges in the cloud that are discussed as follows:

1) Computation eficiency: In data integrity scheme, the data can be pre-processed before outsource into the cloud storage server. The generation of metadata from original data similar to the cloud storage server. In the server end, the computation cost of the proof of possession limits on how regularly the customer can verify or ensure the outsourced data integrity. Data integrity scheme used primitives as metadata that also effects on the computation time.

2) Communication efficiency: The communication efficiency can be described three major aspects in the data integrity scheme: 1) data owner have challenge request for the proof of possession; 2) the challenge response from the cloud storage server for the verification of possession; and overhead occur during the initial transfer of data along the metadata. The metadata utilized the primitives have effects on the communication cost. Algebraic signatures offer the

communication efficiency by using the low network bandwidth during response time and challenge request [41]. The size of response and challenge is usually small by using the Hill cipher and offering the efficient communication.

3) Reduced disk I/O: The overhead in metadata access and block access for the generation of proof on the cloud storage server have derived the efficiency of disk I/O in the data integrity scheme. For the purpose of generating proof to access all blocks that impact on the efficiency of the data integrity scheme and scheme become impractical for employing large datasets. The overall efficiency of disk I/O can influence on following parameters [42], [43].

- The size of the disk in data integrity scheme either employs variable length block size or fixed. The size of the block is small, then the larger the blocks in the file that will influence the preprocessing time in metadata tags generation for all blocks.
- Due to the variable length of data/metadata that cannot be accessed directly a particular block index. It will impact on the disk I/O to increases the process of verification, so the time increases of generating a proof.
- The parameter challenge in a number of blocks has an influence on both the I/O cost and computation cost. The large blocks in a challenge that leads in proof generating time increased.

4) Security: The concerns while designing the data integrity schemes because they are vulnerable to different attacks [44]-[46]. The possible attacks against the schemes are discussed as follows:

- The tag forgery attack is possible through malicious cloud storage provider that tries to hide the data damage of customers and avoid the auditing challenge.
- The pollution attack defines the correct data is employed by the dishonest server in the generation of response against a challenge but it offers corrupted or useless blocks in repair phase.

In the data leak attack, the extraction of stored data by the attacker during the proofing protocol with wiretapping technique.

The data integrity schemes may find difficult or fail to identify the data corruption timely that consequences an unrecoverable damage. The cloud provider ensured to maintain data accuracy and integrity. The cloud computing models explain numerous threats containing the sophisticated insider attack on the data attributes. Software integrity protects the software from the unauthorized modification by intentionally or unintentionally.

B. Confidentiality

Confidentiality refers to keeping the customer's data secret in the cloud computing system and only the authorized customers or systems can able to access the data [49]. Cloud computing provides (e.g. applications and its infrastructures) are basically in the public clouds have more threads on the systems or applications are exposed as compare the hosted in the private data centers. So, it is the fundamental requirement to keep the customer data secret ever the increasing number of applications, customers and devices involved. They create a VPN connection among the enterprise customers and Vertica to the cloud instance and firewall is set for the outside world. Confidentiality is also enhancing by encrypted the data before transfer into cloud storage and TC3 is successfully employed in this approach. Numerous concerns arises regarding the issues of application security and privacy, multi-tenancy, and data remanence [51].

1) Multi-Tenancy: Multi-tenancy refers to the characteristics of cloud resources that shared including the data, memory, networks and programs. Cloud computing is like the business model where the multiple customers can access same shared resources at the application level, host level, and network level. Multi-tenancy is similar to multi-tasking that shares some common processing resources like CPU and it present number of confidentiality and privacy threats.

2) Data Remanence: The data is represented in residual that can be unintentionally removed or erased due to the lack of hardware separation among different customers and

virtual separation of the logical drives on a single cloud infrastructure, it may lead the unintentionally disclose the private data.

3) Application Security and Privacy: Data confidentiality is associated with the user authentication. To protect the customer's account from hackers is a large problem of controlling the access of the objects including problem of controlling the access of the objects including software, devices and memory. The electronic authentication established the confidence of customer identitiesThe possibilities of unauthorized access by the use of vulnerable applications or weak identification that create the issue of data privacy and confidentiality.

C. Availability

Availability in cloud computing including applications and its infrastructure is to ensure that the authorized customers can access the property of system at all time on demand. Cloud computing models (IaaS, PaaS and SaaS) allows its customers to access the services and applications from anyplace at any time. Vendors of cloud computing offers the cloud platform and infrastructure that is based on VM. The Amazon web services offer S3, EC2 that is based on VM called Skytap and Xen provides virtual lab management application depends on the hypervisor (Xen, VMware and Microsoft Hyper-V).

The objectives of distributed system security are as follows:

- To ensure the data confidentiality among the participating systems.
- When add or remove resources on a physical level then maintain the exactly same security level.

- To ensure the availability of data or systems communicated among the participating systems.
- The integrity of data or systems is maintained by preventing any modification or loss from unauthorized access between the participating systems communicated.

software, devices and memory. The electronic authentication established the confidence of customer identities. The possibilities of unauthorized access by the use of vulnerable applications or weak identification that create the issue of data privacy and confidentiality.

D. Trusted Third Party (TTP)

Trusted third party in cryptography helps to facilitate the interaction among the two parties and reviews all crucial operations among them. The cloud computing environment required the TTP services that exhibits to establish the essential trust level and offers an ideal solution to maintain the authenticity, integrity and confidentiality of communication and data. TTP can produce the trusted security domain with the specifically addresses the loss or missing of the traditional security boundary. It is an impartial organization which delivers the confidence of business by technical and commercial security features to electronic transactions [38]. Lightweight directory access protocol has become the vital protocol that supports to access PKI directory services for the Certificate Revocation List (CRL) and employed by web services for the authentication [55]. PKI is coupled with directory can be utilized to distribute: 1) certificate status information (CRL); 2) application certificate such as end-user certificate need to obtain using email before the transfer of encrypted message; and 3) private key, If the users do not use similar machine every day then the portability is needed in the environment. The directory contains the encrypted secret or private key are decrypted using the password given by customer at the remote workstation.

The TTP can depend on following methods are defined as follows:

1) Client-Server Authentication: The certification authority needs to verify the entities or systems that are involved in interaction with the cloud computing environment which includes to certifying virtual servers, network devices, environment users, and physical infrastructure servers. The certification authority of PKI

develops the required strong credentials for the virtual or physical entities that are involved in cloud and security domain are build with specific boundaries. The availability of strongest authentication process in distributed environments is the digital signature that is the combination of Ldap and SSO which ensure the user flexibility and mobility [56]. The authentication of customers is performed transparently and automatically to other devices or servers over the network by signing private key.

2) *Low or high-level confidentiality*: Transmission of data across the network is a challenge due to its continuously rising the threats of data interruption or modification. Due to the deficiency in traditional physical connection, the complexity increases in cloud computing environment that it required not only protection toward cloud traffic but additionally among the cloud hosts. PKI allows by implementing SSL or IPSec protocol for the secure communications. IPSec enables to send or receive the protected packets such as UDP, TCP, ICMP, etc. without any modification and offers authenticity and confidentiality based on the requirement [38], [57].

3) Cryptographic data separation: The protection of sensitive data is essential in the cloud computing environment that established as a crucial factor in the successful SaaS model deployment. Cryptographic separating of the data, computations and processes are hidden or secret using the encryption technique that appears intangible for outsiders and maintains the confidentiality, integrity and privacy of data. Symmetric and asymmetric cryptographic techniques are combined (referred as hybrid cryptography) that can provide the efficiency and security of data [58], [59].

V. CONCLUSION AND FUTURE WORK

Cloud computing is the emerging technology that brings many benefits for its customers, organizations and companies. However, despite bringing several advantages, it raises many security challenges in the adoption of cloud. We explained the detail design of cloud computing architecture in which deployment models, service models, cloud components, and cloud security are explored. This research attempted to present many security challenges, threats, attacks and vulnerabilities in the systems or data during transfer to the cloud. Most of the identified threats can be address by the combination of SSO, LDAP and PKI in cloud computing that is dealing with the authenticity, availability, integrity and confidentiality in communication or data. This research can be further analyzed in future to improve the quality and availability of services that brings the attraction of the customers toward the deployment of cloud computing and develop more customer's trust to the TTP. Also, developing a framework of complete security and privacy trust evaluation management system is a part of cloud computing services which satisfies the security demands.

REFERENCES

[1] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A review of cloud computing," Commun. ACM, vol. 53, no. 4, 2010.

[2] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "NIST cloud computing reference architecture," Proc. IEEE World Congr. Serv., pp. 594–596, 2011.

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Spec. Publ. 800-145, vol. 145, p. 7, 2011.

[4] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," Proc. 10th IEEE Int. Conf. High Perform. Comput. Commun., pp. 5–13, 2008.

[5] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," Proc. 6th Int. Conf. Semant. Knowl. Grid, pp. 105–112, 2010.

[6] D. G. Rosado, R. Gomez, D. Mellado, and E. Fernández-Medina, "Security analysis in the migration to cloud environments," Futur. Internet, vol. 4, pp. 469–487, 2012.

[7] C. Wang, Q. Wang, K. Ren, and W. J. Lou, "Ensuring data storage security in cloud computing," 17th Int. Work. Qual. Serv., pp. 37–45, 2009.

[8] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258, pp. 371–386, 2014.

[9] P. Wilson, "Positive perspectives on cloud security," Inf. Secur. Tech.
Rep., vol. 16, no. 3–4, pp. 97–101, 2011.

[10] L. Savu, "Cloud computing deployment models, delivery models, risks and research challanges," Proceeding IEEE Int. conf. comput. manag., 2011.

[11] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf,

"NIST cloud computing reference architecture," NIST Spec. Publ. 500-292, pp. 1–28, 2011.

[12] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing,"
J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[13] A. paltform computing white Paper, Enterprise Cloud Computing: Transforming IT. 2009.

[14] S. Kaisler, W. H. Money, and S. J. Cohen, "A decision framework for cloud computing," Proceeding IEEE 45th Hawaii Int. Conf. Syst. Sci. A, pp. 1553–1562, 2012.

[15] J. Brodkin, "Seven cloud-computing security risks.," InfoWorld from
IDG, 2008.

[16] A. Macdermott, Q. Shi, M. Merabti, and K. Kifayat, "Detecting intrusions in the cloud environment detecting intrusions in the cloud environment," Proc. 14th Annu. Post- Grad. Symp. Converg. Telecommun. Netw. Broadcast., 2013.

[17] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, pp. 1113–1122, 2011.

[18] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[19] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments,"
Procedia Eng., vol. 15, pp. 2852–2856, 2011.

[20] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," J. Internet Serv. Appl., vol. 1, no. 1, pp. 7–18, 2010.

[21] L. F. B. Soares, D. A. B. Fernandes, J. V. Gomes, M. M. Freire, and P. R. M. Inacio, "Cloud security: state of the art," Secur., Priv. Trust Cloud Syst., pp. 3–44, 2013.

[22] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez,
"An analysis of security issues for cloud computing," J. Internet Serv.
Appl., vol. 4, no. 5, pp. 1–13, 2013.

[23] K. Hashizume, N. Yoshioka, and E. B. Fernandez, "Three misuse patterns for cloud computing," Secur. Eng. Cloud Comput. Approaches
Tools, pp. 36–53, 2013.

[24] T. Garfinkel and M. Rosenblum, "When virtual is harder than real: security challenges in virtual machine based computing environments," Proc. 10th Conf. Hot Top. Oper. Syst., pp. 20–25, 2005.

[25] D. Owens, "Securing elasticity in the cloud," Commun. ACM, vol. 53, no. 6, p. 46, 2010.

[26] M. Al Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," Proc. APSEC Cloud Work. Sydney,
Aust., pp. 1–6, 2010.

[27] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," Proc. Int. Carnahan Conf. Secur. Technol., pp. 35–41, 2010.

[28] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu,
"Multi-Tenancy in cloud computing," IEEE 8th Int. Symp. Serv.
Oriented Syst. Eng., pp. 344–351, 2014.

[29] T. C. Nguyen, W. Shen, Z. Luo, Z. Lei, and W. Xu, "Novel data integrity verification schemes in cloud storage," Comput. Inf. Sci., pp. 115–125, 2014.

[30] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Gov. Inf.., vol. 27, no. 3, pp. 245–253, 2010.

[31] K. Karaoglanoglou and H. Karatza, "Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values," J. Syst. Softw., vol. 84, no. 3, pp. 465–478, 2011.

[32] N. Iltaf, M. Hussain, and F. Kamran, "A mathematical approach towards trust based security in pervasive computing environment," Proceeding Int. Conf. Inf. Secur. Assur., pp. 702–711, 2009.

[33] S. Rizvi, K. Cover, and C. Gates, "A trusted third-party (TTP) based encryption scheme for ensuring data confidentiality in cloud environment," Procedia Comput. Sci., vol. 36, pp. 381–386, 2014.

[34] L. Chen, "Using algebraic signatures to check data possession in cloud storage," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1709–1715, 2013.

[35] E. Esiner, A. Kachkeev, S. Braunfeld, A. Kupcu, and O. Ozkasap, "FlexDPDP: Flexlist-based optimized dynamic provable data possession," *Cryptol. ePrint Arch. Rep. 2013/645*, pp. 1–40, 2013.

[36] G. Ateniese, R. Burns, and J. Herring, "Provable data possession at
untrusted stores," *Proc. 14th ACM Conf. Comput. Commun. Secur.*, pp. 598–610, 2007.

[37] Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang, and C. Xu, "Improved security of a dynamic remote data possession checking protocol for cloud storage," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7789–7796, 2014.

[38] K. Yang and X. Jia, "Data storage auditing service in cloud computing: Challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.

[39] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative integrity verification in hybrid clouds," *Proc. 7th Int. Conf. Collab. Comput. Networking, Appl. Work.*, pp. 191–200, 2011.

[40] S. K. P and R. Subramanian, "An efficient and secure protocol for ensuring data storage security in cloud computing," J. Comput. Sci., vol. 8, no. 6, pp. 261–275, 2011.

[41] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011.

[42] M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, "Above the clouds: A berkeley view of cloud computing," Univ. California,

Berkeley, Tech. Rep. UCB, pp. 7–13, 2009.

[43] M. F. Mushtaq, S. Jamel, and M. M. Deris, "Triangular coordinate extraction (TCE) for hybrid cubes," J. Eng. Appl. Sci., vol. 12, no. 8, pp. 2164–2169, 2017.

[44] Cloud Security Alliance, "Top threats to cloud computing," Cloud Secur. Alliance, pp. 1–14, 2010.

[45] F. S. Al-Anzi, A. A. Salman, N. K. Jacob, and J. Soni, "Towards robust, scalable and secure network storage in cloud computing," Proceeding 4th Int. Conf. Digit. Inf. Commun. Technol. Its Appl., pp. 51–55, 2014.

[46] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," Proc. 16th ACM Conf. Comput. Commun. Secur. - CCS '09, vol. 489, p. 187, 2009.

[47] A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DEPSKY: Dependable and secure storage in a cloud-of-clouds," ACM
Trans. Storage, vol. 9, no. 4, pp. 1–36, 2013.

[48] S. Boeyen and T. Moses, "Trust management in the public-key infrastructure," Entrust seucring Digit. identities Inf., no. January, pp. 1– 36, 2003.

[49] A. Levi and M. U. Caglayan, "The problem of trusted third party in authentication and digital signature protocols," Proc. 12th Int'l Symp.
Comput. Inf. Sci., 1997.

[50] M. S. E. H. Tebaa, "Secure Cloud Computing Through Homomorphic Encryption," Int. J. Adv. Comput. Technol., vol. 5, no. 16, pp. 29–38, 2013.

First Author Dr. Savita, Voc. Teacher (IT) at GGSSS Loharu Distt Bhiwani Haryana, Ph. D. Computer Science & Engg. having an experience of 5 years in the field.

Second Author Satish Kumar, Lecturer in Comp Engg at Govt Polytechnic Loharu Distt Bhiwani Haryana having an experience of 11 years in the field, Qualif. Are B.E. M.A., PGDMC, IEI Membership.