A Review on Various Security Issues in Cloud Computing

Ankita Awasthi
Department of Computer Science & Engineering
School of Research and Technology, People's University Bhopal, India

Abstract— In computer's world recently cloud computing plays vital role. It provides user facilities like cluster of things like package, platform and infrastructure services. Virtualization is that the backbone of cloud resource sharing. Security is additionally a main downside of cloud. Multiple users have their own perception associated with the cloud. By victimisation cloud computing, user will access resources anyplace by victimisation net. Therefore this method is incredibly helpful in user's way of life. One amongst the factors for cloud computing is cloud services that were provided by the cloud (IAAS, PAAS, and SAAS). These services modify users to access infrastructure, platform and package. Even resources square measure allotted to users in step with their needs. however many of us assume it's unsafe to use cloud resources and its services. it's unsafe to use cloud as a result of there's no guarantee of data that is controlled or maintained by the vendors. There square measure some security problems that square measure detected in cloud computing. During this paper, we've got mentioned a couple of problems with cloud computing and therefore the challenges of cloud computing. This paper provides overall investigation of security on information, protection and problems within the cloud. The paper conjointly defines the literature review associated with the cloud computing problems and threats and conjointly the assorted security issues square measure mentioned.

Keywords: Cloud Computing, Cloud Security, IAAS, PAAS, SAAS, NIST, DDOS, IP Spoofing, SLA

I. INTRODUCTION

From the previous construct of preparation models, cloud computing is gaining the recognition. These days, many firms, huge enterprises, area unit enjoying the comforts of cloud services and golf shot their applications and knowledge into it. This ends up in additional potency and effectiveness in developing and preparation and also the burden of buying and maintaining the infrastructure is not any additional a demand. one among the foremost helpful and wide used definition of cloud is authority as "Cloud computing may be a technique that permit convenient, consistent with users demand provides network access to computing resources (e.g., networks, servers, storage, applications, and services) which will be speedily allotted and discharged with least management work. The cloud model consists of 5 characteristics, 3 services, and 4 preparation models." The 3 service models of cloud are: package as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and preparation models are: personal cloud, Community cloud, Public cloud and Hybrid cloud.

But from the user's perspective, cloud computing security is often a significant concern. a number of the protection problems area unit mentioned during this paper. This paper consists of assorted components that has Cloud's applications, its issues, literature review and a few legal problems with cloud computing.

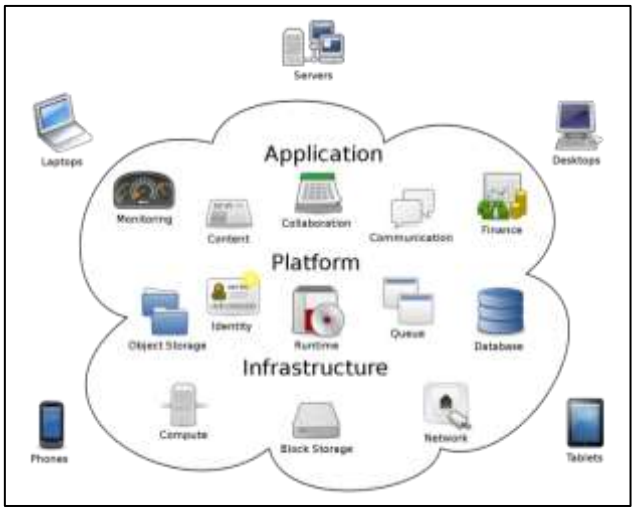

Fig. 1: Cloud computing and its services

II. APPLICATION OF CLOUD COMPUTING

Some of the applications square measure mentioned below in detail:

- By victimization cloud computing users will access its resources and services anytime from anyplace by victimization the web.
- By victimization cloud computing users don't got to purchase infrastructure and applications. as a result of User will access these resources or pay them consistent with their desires. In early time Organizations entirely depend upon systems for process their work and users got to purchase all resources and licenses for an extended time. In Cloud computing user will take the advantages of all resources while not getting it. Payment is completed by pay-per-use policy in cloud computing.
- •Hardware prices square measure reduced by victimization cloud and shoppers haven't any necessities of buying the system with sizable amount of area, magnetic disk etc.
- With cloud computing there's no drawback of area. Thus, users will access, unlimited area and may access it by taking it on rent.
- The cloud system uses the process power of less bestowed system to maximise the speed of the computations. it's varied blessings as compared to ancient techniques, however it additionally has its own problems that square measure mentioned below.

III. ISSUES

The main issue is security and privacy and these concerns are discussed below in detail. Figure 2. Shows various cloud security issues and are explained in detail.

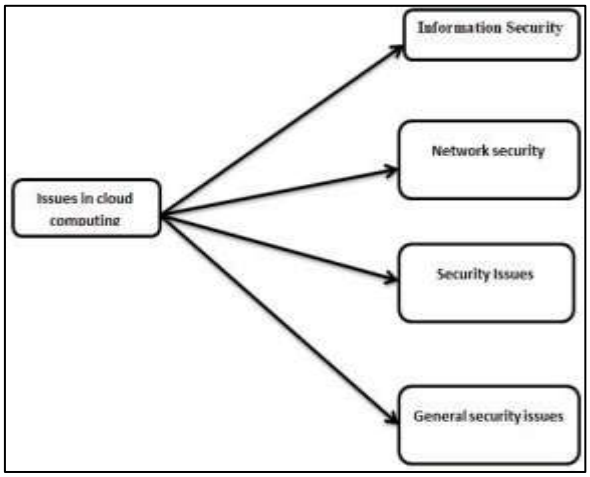

Fig. 2: Issues in cloud computing

A. Information security in cloud computing

It focuses on confidentiality, integrity and availability of data and have no care of the form the data may take. Information Security in cloud computing has various parts that define its issues in detail.

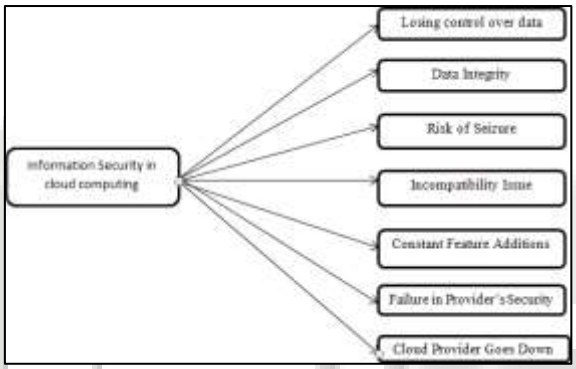

Fig. 3: Types of information security in cloud computing

- Losing control over data: Some banks never want delivered data in the cloud that have no protection in sharing data via communicating with some other system. Amazon S3 APIs gives bucket- and object level access, with defaults that only allow authenticated access by the bucket and/or object creator. Therefore, there is full control of customer over who has access to their resources.
- Data Integrity: Data integrity is a major security concern that means the data alters only in response to authorized actions. It has been observed that the common standard for data integrity does not yet exists. In the area of computing users are needed to accept the underlying premise of trust. In fact, cloud computing facing biggest concern in trust so most of the companies avoiding it for their data.
- Risk of Seizure: In public cloud computing user share the environment in the cloud, may take data at risk of seizure. The Encryption of data is only the security against the risk of seizure for the user.
- Incompatibility Issue: Incompatibility issue is the main concern in cloud computing that means services provided by the cloud service provider may be incompatible with service provided by another cloud service provider. For example, Amazon's "Simple Storage Service" [S3] is not compatible with IBM's Blue Cloud, or Google, or Dell.
- Constant Feature Additions: Constant feature additions always undergo by Cloud applications, and consumer has to keep up to date with application alteration to make sure that these applications are secured. The speed of altering these applications in the cloud affects both the security and Software development life cycle.
- Failure in Provider's Security: The cloud provider normally fails in providing security to the portions of its infrastructure– those results in the compromise of subscribing systems. Cloud consists of various objects, and for this configuration, no cloud can provide much more security. It is expected that User has to trust provider's security. It is very tough to give the details that help to ensure that the right things are being done.
- Cloud Provider goes Down: A number of variants have been noticed: bankruptcy that thinks to take the business in another direction. Due to the actions of another company, subscriber takes the risk of losing access to the production system. It is also a risk that data might not be secured in accordance with the service levels to which they may have been previously committed.

B. Network security in cloud computing

Network security is necessary to secure data while transmitting between a consumer and computer and also between computer to computer. Network security in the cloud is discussed in detail. Figure 4 shows the types of network security in cloud computing that are discussed below.

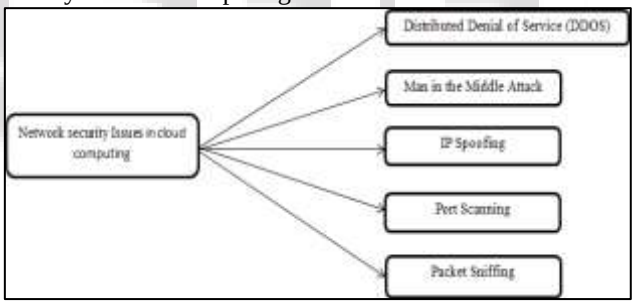

Fig. 4: Types of network security issues in cloud computing

- Distributed Denial of Service Attack: In such type of attack huge amount of network traffic is given to servers and networks and consumers are denied the access to a certain Internet based Service In order to stop hackers from attacking the network, the provider faces blackmail. Proprietary DDOS mitigation methods are widely used. AWS help in providing the application Programming Interface to end users, various resources, best infrastructure that help in making Amazon world's number one retailer.
- Middle Attack: In such type of attack, there is the independent connection of the attacker with the victim. Messages send among them, make them believe that both parties are communicating with each other through secure connection, but in reality the conversation between both of them is controlled and managed by the attacker himself. In such cases, users can use secure APIs for accessing the host certificates before logging on the user first time. Users are guided enough for using SSL for all secure conversations.

- IP Spoofing: In such type of attack, someone tries to use the IP address of another user without his/her permission. Attacker hacks all the confidential data of the user and has an unauthorized way of accessing the system, and can deliver messages to another system with an IP address that shows the message is coming from a trusted user. Spoofed network traffic cannot send by Amazon EC2 instances.
- Scanning of the ports: The cloud provider helps in providing the security group for allowing the flow of traffic from the source to a particular port, then that particular port becomes vulnerable to that scan port. A port is an area which helps in transferring the data in and out, also help in checking open doors for the system. There is no way through which this attack can be stopped because every time searching on the internet opens a port which opens a door for attacking to your system.
- Sniffing of packets: It is a communication with the raw network device for packets that interest you. When the software finds interest in a packet that fulfills a certain procedure, it logs it to a file. The most commonly used procedure is "login" or "password". In promiscuous mode this is an impossible thing to accept or "sniff" traffic that is used for a different virtual instance. The hypervisor never deliver any traffic to users that are not addressed to them.

C. Security issues in cloud computing

Such type of issues is more complex in a virtualized environment as cloud provider have to keep a trail of security on both the tiers, i.e. in virtual machine security and in physical host security. All the virtual machines residing on the host server become impacted if the physical host server's security becomes compromised.

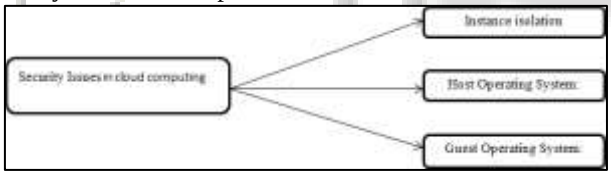

Fig. 5: Security issues

- Isolation of systems: Isolation issues help in protecting various instances which are working over equivalent machine but are separated from each other. In cloud computing, virtualization techniques charge different virtual machines for various organizations for working on the identical platform by sharing the physical resources with each other.
- Host Operating System: Bigger enterprises ought to maintain the business plans which may be used by different authentication for gaining the access for building and configuring different hosts by cloud server.

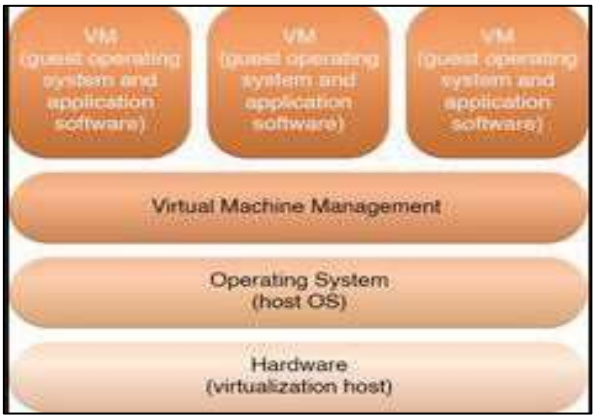

Fig. 6: Host operating system

- Guest Operating System: Consumers are totally responsible for maintaining virtual instances. Consumers have rights to control on resources, applications. AWS has no rights to customer instances and have no permission to log into the guest OS.

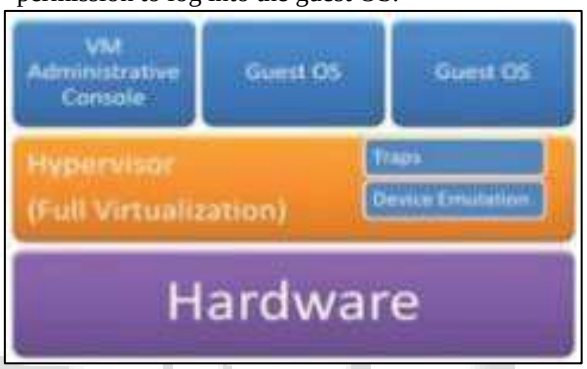

Fig. 7: Guest operating system [26] security is necessary to secure data while transmitting between

D. General Security issues in cloud computing

There are some other general issues of security, they are being deal by cloud computing these days and need to be taken care. These are listed as below.

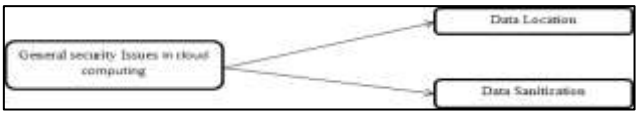

Fig. 8: General issues in cloud

- Data Location: Users using the cloud don't know where their data have been exactly kept or hosted or in which country their data is being residing. Thus, it becomes very difficult for the user to get information about his data that he is storing on the cloud.
- Data Sanitization: In this process sensitive information is being removed from a system which is used to store information. In the environment of a cloud, customers using services are wondering about the information that is placed and how it is maintained by the cloud. So this is also one of issues which should be handled for making the user know about the process.

E. Legal issues

Some of the legal issues of cloud computing are being discussed as under. The legal issues consist of various types such as Jurisdictional Issues and Cloud Stakeholder Rights that are shown in figure.

– Jurisdictional Issues: In a cloud environment, resources are the provided to the users are not fixed to any location or they don't have any specific data center. They are being migrated between different locations during their lifetime. So the decision of where to keep the resources or where to do migration these resources may be based on various factors that may include load balancing, networks, data center for their performance and availability or even on the characteristics of the clients.

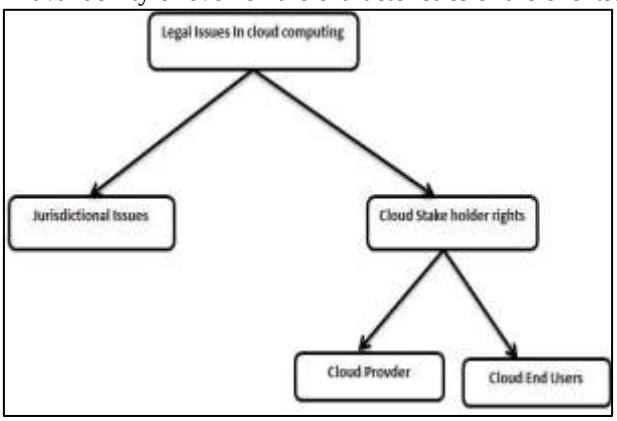

Fig. 9: Legal issues in cloud computing

– Cloud Stakeholder Rights: The cloud stakeholder rights contain 2 main things which are discussed as:
– Cloud Provider: Because of migration of host may change the legality activities taking place on that host, to what extent is she liable for illegal activity and what restrictions should be on the provider that results in such a move?
– Cloud Resource End Users: Users of different resource in a cloud-based system can be expected to know when her activities are illegal?

IV. LITERATURE REVIEW ON CLOUD SECURITY AND THREATS

Literature review of cloud security and threats are discussed in detail in table I that is given below:

Name of author	Description
S. Subashini etal in	The author has done surveys on SQL injection and storage insecurity. The author has further investigated about security and privacy issues in cloud with the special relationship between the cloud provider and cloud user. There are three parties that are joined together in a relationship. Most of the researches which are done earlier discusses about the cloud security from a collective viewpoint outside a cloud.
	recovery.
V. Kavitha et al in	The has discussed about the investigations on security issues in cloud computing delivery models and has given a detailed analysis of different issues related to security in cloud computing [8]. Further author has explored more about the security issues in cloud computing from various perspectives which may include various issues related to security, cloud architecture, various delivery models.
Hamdaqa et al in	The author described that the cloud computing is not considered as a new emerging technology or any concept that came into existence in recent years indeed its having its root from very earlier time when John McCarthy described cloud computing as one of the abilities for providing resources to the user as one of the utility.
Espadas et al in	The author describes cloud computing as the 5th characteristic of cloud that is suggested by the Cloud Alliance. Cloud computing help in modeling different models for policy-driven isolates, governance, service levels, charge back/billing, enforcement and segmentation of different users which are using the cloud services.
Takabi et al in	The author helped in designing and informing about various rules that should be considered for security and various policies of cloud service vendors. However, the author has developed a framework which is self-administered and helps in supplying various services to cloud users with some security and policies which should be maintained by the cloud provider.
Worm et al in	The author successfully helps in providing 3 decision criteria in a cloud that may include executing cost, resting time to deadline and service availability at the decision instant. With the help of such response time and with the availability of services, various dynamic programming is being used for achieving the objectives of cloud, which is necessary for saving results for selecting the best services between all other services available to the user.
Zhou and Mao et al in	The author has proposed an approach for semantic cloud-based web services dealing with Bayesian decision. The authors with the help of Bayesian approach help in anticipating the web service for semantics which may help in discovering the graphs generated on the basis for the use of the implementation in a cloud and also obtaining the relations on the basis of graph which may be formed with the help of the Markov chain.
Sinnema & Deelstra et al in	The author has discussed the basis of modeling variability and cloud feature models which are represented as the mechanisms for explaining about the services and requirements together for preparing definite cloud service selection process.

Table I: Literature Review on Cloud Security and Threats

V. CONCLUSION

The phenomenon of cloud is making huge engrossment in everywhere due to its features like scalability, small workload for customers, quick and comfortable access of resources and cheaper cost. It provides various benefits to the user. Users are getting to know about this technique from various sources. Many consumers have this perception that cloud is not a secure area to work on, though some are finding it much more secure than other security policies, mainly those areas which don't have enough resources for securing themselves. Many big organizations and government organizations are holding back to the cloud environment because they feel it unsafe for storing their data. So if cloud computing has to get accepted by consumers, or by other areas to create big organizations, it should develop some skilled standardization of security and also certification should be done by third parties for ensuring that standards are properly met.

REFERENCES

[1] Atayero and O. Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption," J. Emerg. Trends Comput. Inf. Sci., vol. 2, no. 10, pp. 546–552, 2011
[2] Ahmad and A. Khandekar, "Homomorphic Encryption Method Applied to Cloud Computing," Int. J. Inf. Comput. Technol., vol. 4, no. 15, pp. 1519–1530, 2014.
[3] Boneh, "Evaluating 2-DNF Formulas on Ciphertexts," pp. 1–16, 2006.
[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," Proc. - IEEE INFOCOM, 2010.
[5] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, 2012.
[6] C. Fontaine and F. Galand, "A Survey of Homomorphic Encryption for Nonspecialists," vol. 2007, 2007.
[7] C. Hay, K. Nance, and M. Bishop, "Storm clouds rising: Security challenges for IaaS cloud computing," Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 1–7, 2011.
[8] D. Naccache and J. Stern, "A New Public-Key Cryptosystem Based on Higher Residues," pp. 59–66, 1998.
[9] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 Int. Conf. Comput. Sci. Electron. Eng., no. 973, pp. 647–651, 2012.
[10] D. Hrestak and S. Picek, "Homomorphic encryption in the cloud," 2014 37th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2014 - Proc., no. 2, pp. 1400–1404, 2014.
[11] Data, "Lecture 1 Homomorphic encryption Related cryptographic notions," pp. 1–6, 2013.
[12] Ertaul, S. Singhal, and G. Saldamli, "Security Challenges in Cloud Computing," Secur. Manag., pp. 36–42, 2010.
[13] Journal and A. Technology, "Secure Ranked Keyword Search Over Cloud Data," vol. 2, no. 8, pp. 39–43, 2014.
[14] Kerschbaum, "Outsourced Private Set Intersection Using Homomorphic Encryption," 2012.
[15] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," pp. 223–238, 1999.
[16] Q. Wang, S. Member, C. Wang, S. Member, and K. Ren, "Enabling Public Auditability and Data Dynamic in Cloud Computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2012.
[17] R. Kandukuri, R. P. V., and A. Rakshit, "Cloud Security Issues," 2009 IEEE Int. Conf. Serv. Comput., pp. 517–520, 2009.
[18] Ren and C. Wang, "Security Challenges for the Public Cloud," pp. 69–73, 2012.
[19] R. Chow et al., "Controlling data in the cloud," Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW '09, p. 85, 2009.
[20] R. Shruthi, P. Sumana, and A. K. Koundinya, "Performance Analysis of Goldwasser-Micali Cryptosystem," vol. 2, no. 7, pp. 2818–2822, 2013.
[21] S. Suganya and P. Damodharan, "Enhancing security for storage services in cloud computing," Curr. Trends Eng. Technol. (ICCTET), 2013 Int. Conf., vol. 3, no. 6, pp. 396–398, 2013.
[22] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing.pdf," Ieee Infocom, pp. 1–9, 2010.
[23] Tebaa, S. E. L. Hajji, and A. E. L. Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security," vol. I, pp. 8–11, 2012.
[24] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," vol. I, pp. 469–472, 1985.
[25] Van Dijk and C. Gentry, "Fully Homomorphic Encryption over the Integers," pp. 1–28, 2010.
[26] Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, 2010.
[27] X. Yi, R. Paulet, and E. Bertino, "Homomorphic Encryption and Applications," 2014.
[28] X. Sun, L. Zhou, Z. Fu, and J. Wang, "Privacy-preserving multi- keyword ranked search over encrypted cloud data supporting dynamic update," Int. J. Secur. its Appl., vol. 8, no. 6, pp. 1–16, 2014.
[29] Z. Shen, "The Security of Cloud Computing System enabled by Trusted Computing Technology," Signal Processing, vol. 2, pp. 11– 15, 2010.

