Security Issues in Cloud Computing

ABSTRACT-- Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it's important to require advantages of cloud computing by means of deploying it in diversified sectors, the safety aspects during a cloud based computing environment remains at the core of interest. Cloud based services and repair providers are being evolved which has resulted during a new business trend supported cloud technology. With the introduction of various cloud based services and geographically dispersed cloud service providers, sensitive information of various entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security isn't robust and consistent, the pliability and advantages that cloud computing has got to offer will have little credibility. This paper presents a review on the cloud computing concepts also as security issues inherent within the context of cloud computing and cloud infrastructure..

KEYWORDS-- Cloud computing, cloud service, cloud&security, network ,distributed computing, security.

I. INTRODUCTION

Cloud computing is a new revolution in the era of technology. This paradigm adds new concepts, techniques and approaches to the computing science. In Cloud, software and its data are created and managed virtually for the users and only accessible via a specific Cloud's software, platform or infrastructure. Earlier it was just imagination to rent resources, information and software in order to operate, run and enhance their devices and programs. Now, it is possible to rent whatever resources you like so that this dream is now realized. Cloud computing may be a model for convenient and on-demand network access to a shared pool of configurable computing resources which will be rapidly provisioned and released with minimal management efforts. Cloud computing are often defined as "Cloud may be a parallel and distributed computer system consisting of a set of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources supported service-level agreements (SLA) established through negotiation between the service provider and consumers". It is a method of computing where IT-related capabilities are provided to consumer as "service" instead of a product using the web . Main goal of the cloud computing is to supply scalable and cheap on-demand computing infrastructures with good quality of service levels. Many developers of cloud-based applications struggle to incorporate security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities.

II. CLOUD COMPUTING INFRASTRUCTURE

The term cloud computing is quite an idea which may be a generalized meaning evolved from distributed and grid computing. Cloud computing is described because the offspring of distributed and grid computing by some author. Straightforward meaning of cloud computing refers to the features and scenarios where total computing might be done by using someone else's network where ownership of hardware and soft resources are of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially within the sort of distributed computing; though this is not apparent or by its definition of cloud computing, don't essentially need to be apparent to the users.

In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service within the cloud. Where the previous one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with variety of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is quite an idea , so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized sort of grid and distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion. In a pervasive meaning within the context of computer

networks, infrastructure might be thought of because the hardware also as their alignment where platform is that the OS which acts as the platform for the software. Thus the concept of cloud based services is hierarchically built from bottom to top within the order of IaaS, PaaS and SaaS. This is merely the extent of abstraction that defines the extent to which an end-user could 'borrow' the resources starting from infrastructure to software – the core concern of security and therefore the fashion of computing aren't suffering from this level of abstraction. As a result, security is to be considered within any sort of cloud computing no matter flavour, hierarchy and level of abstraction. Virtualization is an inevitable technology that's highly including the concept of cloud computing– it's the virtualization technology that enhances cloud services specially within the sort of PaaS and SaaS where one physical infrastructure contains services or platforms to deliver variety of cloud users simultaneously. This results in the addition of total security aspects of virtualization technology on top of the prevailing security concerns and problems with cloud computing. Figure 1 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture.

The illustration of cloud architecture in figure 1 is a simplest one where few complex characteristics of cloud computing (e.g. redundancy, server replication, and geographic dispersion of the cloud providers' network) are not shown – the purpose of the illustration is to establish the arrangement that makes the concept of cloud computing a tangible one. The network architecture is self-explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing concept presented earlier. One notable part from the architecture is that, while the cloud users are clearly identified and named accordingly due to their remote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud service provider's network in the scenario. It is arguable whether the LAN users in figure 1 are cloud users or not. Such room for argument could exist due to the phrase 'cloud computing' being a concept rather than a technical terminology. If the definition of cloud computing is taken to have essential arrangements of being the servers located remotely that are accessed through public infrastructure (or through cloud), then the LAN users in figure 1 may not be considered as the cloud users in the context. With respect to distributed and grid computing as the mother technology that define the infrastructural approach to achieve cloud computing, the LAN users in the scenario are essentially the cloud users when they use the cloud services offered by the servers; the LAN users in this perspective are essentially using resources that are 'borrowed' from the servers on an on-demand basis.

As depicted in figure 2, the technical details, arrangements and management of the cloud service providers' network is transparent to the cloud user. From the end of the cloud user, the service from the provider comes in the form of SaaS, PaaS or IaaS where the cloud user has no intention or worry about what goes on in the internal arrangement of the cloud service providers' network. Any disruption of any form for whatever is the reason, deem to the cloud users either as service unavailability or quality deterioration – its affect and ways to counter this disruption is a critical part for the cloud infrastructure. Security issues might play a stimulating role as a driving factor for any aforementioned disruption.

III. CLOUD COMPUTING SECURITY

A. Layered Framework for Cloud Security

There is a layered framework is available that assured security in cloud computing environment. It consists of four layers. First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer, this layer combining both hardware and software solutions in virtual machines to handle problems. However, there are several groups working and interested in developing standards and security for clouds. The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them. CSA gathers solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. Another group is Open Web Application Security Project (OWASP). OWASP maintains a list of vulnerabilities to cloud based or Software as a Service deployment models which is updated as the threat landscape changes.

B. Components Affecting Cloud Security

There are numerous security issues for cloud computing as it encompasses many technologies including virtualization, resource allocation, transaction management, cloud networks, databases, operating systems, load balancing, concurrency control and memory management.

C. Security Issues Faced By Cloud Computing

Cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. Cloud computing infrastructures use new technologies and services, most which have not been fully evaluated with respect to security. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. In other way, we can understand it by below given arguments: Security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users' personal data security is thus a crucial concern in a cloud computing environment. In terms of customers' personal or business data security, the strategic policies of the cloud providers are of highest significance (Joint & Baker, 2011) as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service for the reason that it is directly related to the credibility and authenticity of the cloud service providers. Trust establishment might become the key to establish a successful cloud computing environment. The provision of trust model is essential in cloud computing as this is a common interest area for all stakeholders for any given cloud computing scenario. Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies.Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent. All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some threats in this category are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDOS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure (Dou, Chen & Chen, 2013). The well-known DDOS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this. The security of virtual machine will define the integrity and level of security of a cloud environment to greater extent. Accounting & authentication as well as using encryption falls within the practice of safe computing - they can be well considered as part of security concerns for cloud computing. However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system might pose security threat and concerns which, of course, is a security risk. Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint. Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing. Any security tools or other kinds of software

used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment.

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber-attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach. The approach by which cloud computing is done has made it prone to both information security and network security issues. Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects. Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one. Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment.

The facets from which the security threat might be introduced into a cloud environment are numerous ranging from database, virtual servers, and network to operating systems, load balancing, memory management and concurrency control. Data segregation and session hijacking are two potential and unavoidable security threats for cloud users. One of the challenges for cloud computing is in its level of abstraction as well as dynamism in scalability which results in poorly defined security or infrastructural boundary. Privacy and its underlying concept might significantly vary in different regions and thus it may lead to security breach for cloud services in specific contexts and scenarios (Chen & Zhao, 2012). Data loss and various botnets can come into action to breach security of cloud servers. Besides, multi-tenancy model is also an aspect that needs to be given attention when it comes to security. Security in the data-centres of cloud providers are also within the interests of security issues, as a single physical server would hold many clients' data making it a common shared platform in terms of physical server or operating system. The storage security at the cloud service providers data centres are also directly linked with the security of the cloud services. All the traditional security risks are thus applicable with added degree of potency in a cloud infrastructure which makes the ongoing success of cloud computing a quite challenging one. Confidentiality, availability and integrity are the generalized categories into which the security concerns of a cloud environment falls. Threats for a cloud infrastructure are applicable both to data and infrastructure.

Different modes of data transfer and communication means (e.g. satellite communication) might need to take into account. Huge amount of data transfer is a common anticipation in a cloud environment, the communication technology used along with the security concerns of the adapted communication technology also becomes a security concern for the cloud computing approach. The broadcast nature of some communication technology is a core concern in this regard. Cloud environment is associated with both physical and virtual resources and they pose different level of security issues – having no sophisticated authentication mechanism to fully address the security threats is an existing problem for cloud computing. It has mainly resulted in the situations where grid computing has been taken as an embedded part of cloud computing. As the virtualized resources are highly coupled with a cloud infrastructure, intrusion related security concerns are of utmost priority as part of security issues. Arbitrary intermittent intrusion needs to be monitored in the operational context of a cloud computing infrastructure where the severity of possibility for a virtual machine to be compromised is to be taken into account (Arshad, Townsend & Xu, 2013). Some authors have argued that using Internet technologies is not a must for cloud computing but the cost efficiency and globalization trends will enforce and motivate almost all the businesses to admit Internet and associated technologies to be the ultimate means towards cloud computing approach. As a result, total Internet related security concerns are anticipated to be automatically added on top of the cloud-specific security issues. Bringing portability is one of the means to make cloud services flexible. The portability of cloud services would also be associated with security concerns. Cloud portability enables the cloud users to switch among different cloud service providers without being affected with the necessity to change the ways to accomplish tasks in different ways. It is a clear provision on bargaining power for the cloud users; but at the same time, the security issues with cloud portability are to be counted. Cloud portability might bring severe degree of API based security threats.

The wide transition to mobile computing practices in recent years has made it imperative to include mobile computing and its associated technologies as an essential part of cloud computing. Resource

scarcity as well as other constraints of mobile computing is barriers to cloud computing. The demand of huge data processing is a problem for mobile end-user devices which has been further complemented by the security concerns of mobile cloud computing. For mobile cloud computing, the device level limitations has inspired researchers to suggest the inclusion of another level of cloud termed as 'mobile cloud' to aid the processing of the specific computing and processing for mobile computing devices. The earlier explained broadcast nature of satellite communication and related security issues are equally applicable to the mobile cloud computing due to its being wireless communication. Besides, the addition of mobile cloud into the perspective would add another cloud with all its security issues for a service provider having both mobile cloud and conventional cloud. The addition of mobile cloud in the scenario would boost performance, but it would also add another layer of security issue not only to the mobile cloud users, but also to the total infrastructure of the cloud service provider. The hierarchical arrangement of cloud computing facilitates different level of extensibility for the cloud users with varying degree of associated security issues. Security issues for cloud computing are described by some authors as an obvious one due to its nature. In a business model, the risks for the consumers are related to and dependent on the relevant approaches and policies of the cloud service providers the consumers are dealing with. Using cloud products or services may lead to security concerns for the consumers if they are not well aware with the type and particulars of the products or services they are to procure or to use in a cloud environment; this is also related to the cloud providers' identity and reliability. One of the inherent problems in this context is that, the consumers might normally not be able to identify or foresee all the risks involved in the specific cloud transaction they are dealing with or involved in.

IV. SOLUTION FOR CLOUD SECURITY ISSUES

There are some cloud security solutions, that providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

Trust between the Service provider and the customer is one of the main issues cloud computing. Service Level Agreement (SLA) is the only legal document between the customer and service provider. Which contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do.

Legal Issues is also one of the major problems, the laws vary from country to country, and users have no control over where their data is physically located. Regulatory measures likes, privacy laws and data security laws that cloud systems need to follow.

Preserving confidentiality and Integrity is one of the major issues. Data encryption preventing the improper disclosure of information.

Authenticity may varies with varying amount of users rights. Sometimes there would be a user with a limited set of rights might need to access a subset of data, and might also want to verify that the delivered results are valid and complete Solution for such problems is to use digital signatures. Then the problem with digital signatures is that not all users have access to the data superset, therefore they cannot verify any subset of the data even if they are provided with the digital signature of the superset; and too many possible subsets of data exist to create digital signatures for each. Solutions to this problem is to provide customers with the supersets signature and some metadata (verification objects) along with the query results.

Data Splitting is also a solution for cloud security issues. Here the data split over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original.

Data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumers data.

Make sure the consumer's access devices or points such as personal computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. Access to the device by an unauthorized user can cancel even the best security protocols loss of an endpoint access device in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

Data Access Monitoring have to assure about whom, when and what data is being accessed for what purpose.

Cloud service provider must share diagrams or any other information or provide audit records to the consumer or user. Provider must verify the proper deletion of data from shared or reused devices. Cloud service providers must give enough details about fulfilment of promises, break remediation and reporting contingency.

V. CONCLUSION

Cloud computing by itself is in evolving stage and hence the security implications in it aren't complete. It is emerging as the various organizations that are developing cloud services are evolving. It is evident that the Even the leading cloud providers such as Amazon, Google etc. are facing many security challenges and are yet to stabilize. Achieving complete solution for legal issues is still a question. With this level of issues in cloud computing, decision to adopt cloud computing in an organization could be made only based on the benefits to risk ratio.

Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest comes when the differences between actual cloud security and virtual machine security comes. Research should be centre on these gaps and differences and its removal. Main goal of cloud computing is to securely store and manage the data in cloud. One solution for cloud security issues is to produce the framework might be developing a way to monitor the clouds management software, and another might be development of isolated processing for specific clients‟ applications. It is useful to track the clients behaviour and monitored for instance whether client allow the updating anti-virus software definitions , or ,automated patching software to run, or whether client understand how to make safe their virtual machines in the cloud.

REFERENCES

1. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006.
2. Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
3. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009.
4. Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
5. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103.
6. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.