ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering
Tome VII [2014] Fascicule 4 [October – December]
ISSN: 2067 – 3809

1. Rohit BHADAURIA, 2. Rituparna CHAKI,
3. Nabendu CHAKI, 4. Sugata SANYAL

A SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING

1. School of Electronics and Communications Engineering, Vellore Institute of Technology, Vellore, INDIA
2. West Bengal University of Technology, BF-142, Sector III, Salt Lake, Kolkata, INDIA
3. Department of Computer Science & Engineering, University of Calcutta, Kolkata, INDIA
4. Corporate Technology Office, Tata Consultancy Services Mumbai, INDIA

Abstract: *Cloud Computing holds the potential to eliminate the requirements for setting up of high-cost computing infrastructure for the IT-based solutions and services that the industry uses. It promises to provide a flexible IT architecture, accessible through internet for lightweight portable devices. This would allow multi-fold increase in the capacity or capabilities of the existing and new software. In a cloud computing environment, the entire data reside over a set of networked resources, enabling the data to be accessed through virtual machines. Since these data-centres may lie in any corner of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and taken care of. Also, one can never deny the possibility of a server breakdown that has been witnessed, rather quite often in the recent times. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario. This extensive survey paper aims to elaborate and analyze the numerous unresolved issues threatening the Cloud computing adoption and diffusion affecting the various stake-holders linked to it.*

Keywords: *Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Interoperability, Denial of Service (DoS), Distributed Denial of Service (DDoS), Mobile Cloud Computing (MCC)*

1. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter [23, 32].

*A plethora of definitions have been given explaining the cloud computing. Cloud Computing has been defined as the new state of the art technique that is capable of providing a flexible IT infrastructure, such that users need not own the infrastructure supporting these services. This integrates features supporting high scalability and multi-tenancy. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. According to the different types of services offered, cloud computing can be considered to consist of three layers. IaaS or Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service. PaaS – the Platform as a Service (PaaS) layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. SaaS - Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand [5]. **SaaS** ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock" [3]. Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance.*

© copyright Faculty of Engineering - Hunedoara, University POLITEHNICA Timisoara

*In the **Platform as a service approach (PaaS)**, the offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons [34].*

***Infrastructure as a service (IaaS)** refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged for on a pay-per-use basis. The resources are all virtual machines, which has to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information.*

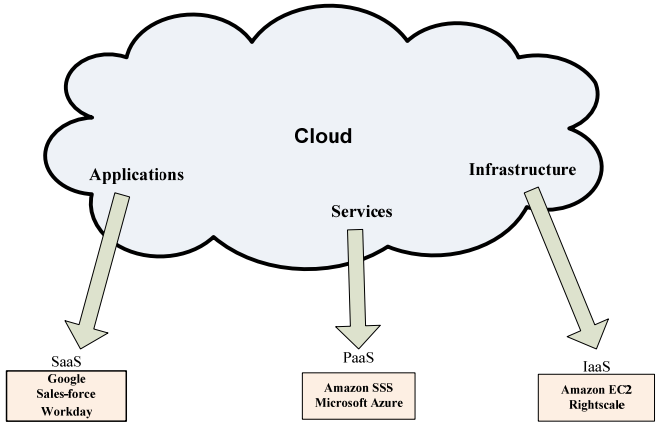

Fig.1. A simple cloud computing model with the three basic cloud services involved

Fig.1 shows the basic cloud architecture depicting the various service providers associated with different elements of cloud. Irrespective of the above mentioned service models, cloud services can be deployed in four ways depending upon the customers' requirements:

a. *Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party [70]. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources through the internet from an off-site service provider. Wastage of resources is checked as the user pays for whatever they use.*
b. *Private Cloud: Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider [70]. This uses the concept of virtualization of machines, and is a proprietary network*
c. *Community cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider.*
d. *Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other.*

Moreover, with the technological advancements, we can see derivative cloud deployment models emerging out of the various demands and the requirements of users. A similar example being a virtual-private cloud wherein a public cloud is used in a private manner, connected to the internal resources of the customer's data-centre [55]. With the emergence of high-end network access technologies like 2G, 3G, Wi-Fi, Wi-Max etc and feature phones, a new derivative of cloud computing has emerged. This is popularly referred as "Mobile Cloud Computing (MCC)". It can be defined as a composition of mobile technology and cloud computing infrastructure where data and the related processing will happen in the cloud only with an exception that they can be accessed through a mobile device and hence termed as mobile cloud computing [43]. It's becoming a trend now-a-days and many organizations are keen to provide accessibility to their employees to access office network through a mobile device from anywhere.

Recent technical advancements including the emergence of HTML5 and various other browser development tools have only increased the market for mobile cloud-computing. An increasing trend towards the feature-phone adoption [43] has also ramped up the MCC market.

Cloud Computing distinguishes itself from other computing paradigms like grid computing, global computing, internet computing in the various aspects of On Demand Service Provision, User Centric Interfaces, guaranteed QoS, Autonomous system [25], etc. A few state of the art techniques that contribute to the cloud computing are:

- ✓ ***Virtualization:*** *It has been the underlying concept towards such a huge rise of cloud computing in the modern era. The term refers to providing an environment able to render all the services, being supported by a hardware that can be observed on a personal computer, to the end users. The three existing forms of virtualization categorized as: Server virtualization, Storage virtualization and Network virtualization have inexorably lead to the evolution of Cloud computing. As for example, a number of underutilized physical servers may be consolidated within a smaller number of better utilized severs [8].*
- ✓ ***Web Service and SOA:*** *Web services provided services over the web using technologies like XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). The service organisation inside a cloud is managed in the form of Service Oriented Architecture (SOA) and hence we can define SOA as something that makes use of multiple services to perform a specific task.*
- ✓ ***Application Programming Interface (API):*** *Without API's it's hard to believe the existence of cloud computing. The whole bunches of cloud services depend on API's and allow deployment and configuration through them. Based on the API category used viz. Control, Data and Application API's different functions are being controlled and services rendered to the users.*

Web 2.0 and mash-up: *Web 2.0 has been defined as a technology, enabling us to create web pages that don't limit a user to viewing only; in fact it allows the users to make dynamic updates as well. It enables the usage of World Wide Web technology towards a more creative and a collaborative platform. Mash-up is a web application that combines data from more than one source into a single integrated storage tool.*

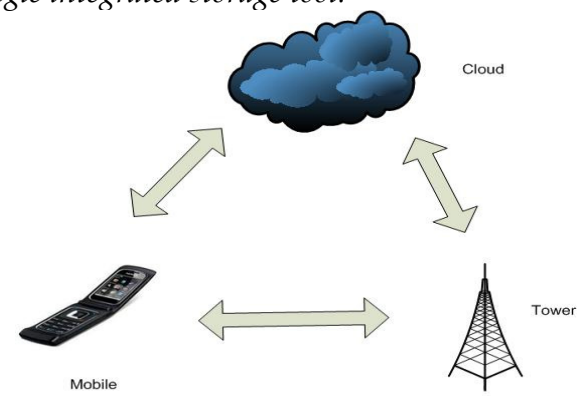

Fig. 2. A Mobile Cloud Computing Scenario

These were the few technological advances that led to the emergence of Cloud Computing and enabled a lot of service providers to provide the customers a hassle free world of virtualization fulfilling all their demands. The prominent ones are: Amazon-EC2 [19] (Elastic Compute Cloud), S3 (Simple Storage Service), SQS (Simple Queue Service), CF (Cloud Front), SimpleDB, Google, Microsoft, ProofPoint, RightScale, Salesforce.com, Workday, Sun Microsystems etc and each of them are categorised either as one of the three main classifications based on the cloud structure they provide: private, public and hybrid cloud. Each of the above mentioned cloud structure has its own limitations and benefits.

The enormous growth in this field has changed the way computing world was looked at. The IT sector has witnessed the change in the way situations were handled. However, there are issues that are same as forever and yet more compelling now. The amount of significant resources available at very low price is acting as a catalyst to distributed attacks on confidential information.

With an avalanche rise towards the deployment of Cloud Computing, the ever consistent security and privacy issues have become more sophisticated, more distributed in the sense that the user section for such services is growing by leaps and bounds [11, 39]. With the increase of on-demand application usage, the potential of cyber attacks also increases. Individual users have to frequently provide online information about their identification, and these could be used by attackers for identity theft. In order to maintain various security and privacy issues like: confidentiality,

operational integrity, disaster recovery and identity management, following schemes should be deployed at least to ensure data security [27] to some extent like:

- ✓ *An encryption scheme to ensure data security in a highly interfering environment maintaining security standards against popular threats and data storage security.*
- ✓ *The Service Providers should be given limited access to the data, just to manage it without being able to see what exactly the data is.*
- ✓ *Stringent access controls to prevent unauthorized and illegal access to the servers controlling the network.*
- ✓ *Data backup and redundant data storage to make data retrieval easy due to any type of loss unlike the recent breakdown issues with the Amazon cloud.*
- ✓ *Distributed identity management and user security is to be maintained by using either Lightweight Directory Access Protocol (LDAP), or published APIs (Application Programming Interfaces) to connect into identity systems.*
- ✓ *An important aspect of cloud computing is that it does give rise to a number of security threats from the perspective of data security for a couple of reasons. Firstly, the traditional techniques cannot be adopted as these have become quite obsolete with respect to the ever evolving security threats and also to avoid data loss in a cloud computing environment. The second issue is that the data stored in the cloud is accessed a large number of times and is often subject to different types of changes. This may comprise of bank accounts, passwords and highly confidential files not to be read by someone else apart from the owner. Hence, even a small slip may result in loss of data security.*

This paper is aimed at developing an understanding of the manifold security threats that do hamper the security and privacy of a user. Characteristics of a secure cloud infrastructure (public or private) will be discussed as also the challenges waiting and ways to solve them.

2. BARRIERS TO CLOUD COMPUTING

In spite of being a hot topic, there are certain aspects behind the fact that many organizations are yet not confident of moving into the cloud. Certain loopholes in its architecture have made cloud computing vulnerable to various security and privacy threats [62]. A few issues limiting the boundaries of this transformational concept are:

2.1. Privacy and Security

The fundamental factor defining the success of any new computing technology resides on the term how much secure it is [24, 65, 54]. Whether the data residing in the cloud is secure to a level so as to avoid any sort of security breach or it is more secure to store the data away from cloud in our own personal computers or hard drives? At-least we can access our hard drives and systems whenever we wish to, but cloud servers could potentially reside anywhere in the world and any sort of internet breakdown can deny us access to the data lying in the cloud. The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately stored. There have been instances when their security has been invaded and the whole system had been down for hours. At-least half a dozen of security breaches occurred last year bringing out the fundamental lapses in the security model of major CSPs. With respect to cloud computing environment, is defined as "the ability of an entity to control what information it reveals about itself to the cloud/cloud SP, and the ability to control who can access that information".[11] discusses the standards for collection, maintenance and disclosure of personality identifiable information. Information requiring privacy and the various privacy challenges need the specific steps to be taken in order to ensure privacy in the cloud as discussed in [4 , 40].

In case of a public-cloud computing scenario, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. A public cloud acts as a host of a number of virtual machines, virtual machine

monitors, supporting middleware [13] etc. The security of the cloud depends on the behaviour of these objects as well as on the interactions between them. Moreover, in a public cloud enabling a shared multi-tenant environment, as the number of users is increasing, security risks are getting more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection [61]. Because of the multifarious security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to public cloud in future if needed [63].

Emergence of cloud computing owes significantly to mashup. A mashup is an application that combines data, or functionality from multiple web sources and creates new services using these. As these involve usage of multiple sub-applications or elements towards a specific application, the security challenges are diverse and intense. Based on this idea, a secure component model addressing the problem of securing mash-up applications has been proposed in [71]. Also, privacy needs to be maintained as there are high chances of an eavesdropper to be able to sneak in.

2.2. Performance, Latency and Reliability

Latency [28, 60] has always been an issue in cloud computing with data expected to flow around different clouds. The other factors that add to the latency are encryption and decryption of the data when it moves around unreliable and public networks, congestion, packet loss and windowing. Congestion adds to the latency when the traffic flow through the network is high and there are many requests (may be of same priority) that need to be executed at the same time. Windowing is another message passing technique whereby the receiver has to send a message to the sender that it has received the earlier sent packet and hence adds to the network latency. Moreover, the performance of the system is also a factor that should be taken into account. Sometimes the cloud service providers' run short of capacity either by allowing access to too many virtual machines or reaching upper throughput thresholds on their Internet links because of high demand arising from the customer section. This hurts the system performance and adds to latency of the system.

2.3.Portability and Interoperability

Organizations may need to change the cloud providers and there have been cases when companies can't move their data and applications if they find another cloud platform they like better than the one they are using. Also, some companies use different cloud platforms for different applications based on their requirements and the services provided by the cloud service providers (CSPs). In some cases, different cloud platforms are used for a particular application or different cloud platforms have to interact with each other for completing a particular task. The internal infrastructure of the organization is needed to maintain a balance to handle the interoperability between different cloud platforms [22]. The risk of outsourced services going out of control is too much in a hybrid public and private cloud environment. All data has to be encrypted for proper security, and key management becomes a difficult task in such situations [6]. The users have actually no idea of where their information is stored [9]. Normally, a user's data is stored in a shared environment, along-with other user's data. The issue of inter-security handling becomes important in such cases. A cloud security management model is discussed in [6] to serve as a standard for designing cloud security management tools. The model uses four interoperating layers for managing the cloud security.

Thus we see that although the buzz of cloud computing prevails everywhere because of the multi-fold features and facilities provided by it, still there are issues that are needed to be solved in order to reach the landmarks set by it as to gain access to the hardware and application resources for a better functioning IT world.

2.4. Data-Breach through Fibre Optic Networks

It has been noticed that the security risks for the data in transit has increased over the last few years. Data transitioning is quite normal now-a-days and it may include multiple data-centres and other cloud deployment models such as public or private cloud. Security of the data leaving a data-centre to another data-centre is a major concern as

it has been breached quite a number of times in the recent times.

This data transfer is done over a network of fibre-optic cables which were considered to be a safe mode of data-transfer, until recently an illegal fibre eavesdropping device in Telco Verizon's optical network placed at a mutual fund company was discovered by US Security forces [44]. There are devices that can tap the data flow without even disturbing it and accessing fibre, through which data is being transferred. They generally are laid underground and hence it should not be a tough job accessing these fibre-optic cables. And hence it becomes quite important a factor to ensure data security over the transitioning networks.

2.5. Data Storage over IP Networks

Online data storage is becoming quite popular now-a-days and it has been observed that majority of enterprise storage will be networked in the coming years, as it allows enterprises to maintain huge chunks of data without setting up the required architecture. Although there are many advantages of having online data storage, there are security threats that could cause data leakage or data unavailability at crucial hour. Such issues are observed more frequently in the case of dynamic data that keeps flowing within the cloud in comparison to static data. Depending upon the various levels of operations and storage provided, these networked devices are categorized into SAN (Storage area network) and NAS (network-attached storage) and since these storage networks reside on various servers, there are multiple threats or risks attached to them. The three threat zones that may affect and cause the vulnerability of a storage network have been discussed in [62, 66].

Besides these, from them a mobile cloud computing scenario, we may see that unlike cloud computing there are several additional challenges that need to be addressed to enable MCC reach its maximum potential:

- ✓ *Network accessibility: Internet has been the major factor towards the cloud computing evolution and without having the network access it won't be possible to access the internet and hence the inability to access the mobile cloud limiting the available applications that can be used.*
- ✓ *Data Latency: Data transfer in a wireless network is not as continuous and consistent as it is in case of a dedicated wired LAN. And this inconsistency is largely responsible for longer time intervals for data transfer at times. Also, the distance from the source adds up to the longer time intervals observed in case of data transfer and other network related activities because of an increase in the number of intermediate network components.*
- ✓ *Dynamic Network monitoring and Scalability: Applications running on mobiles in a mobile cloud computing platform should be intelligent enough to adapt to the varying network capacities and also they should be accessible through different platforms without having suffered any loss in the data. Sometimes, a user while working on a smart phone may need to move on to a feature phone and when (s)he accesses the application which (s)he was working on through her/his smart phone, (s)he should not face any data loss.*
- ✓ *Confidentiality of mobile cloud-based data sharing: The confidential data on mobile phones using cloud-based mobile device support might become public due to a hacked cloud provider. The root-level access to cloud services and information can be easily accessed from a stolen mobile device. If the stolen device belongs to a system administrator, they may even provide direct and automated access to highly confidential information.*
- ✓ *Better access control and identity management: As cloud computing involves virtualization, the need of user authentication and control across the clouds is high. The existing solutions are not able to handle the case of multiple clouds. As multiple users' data are stored by a single hypervisor, specific segmentation measures are needed to overcome the potential weakness and flaws in hypervisor platform.*

Apart from the above mentioned network related challenges there are somewhat different security challenges in a mobile cloud computing environment. With applications lying in a cloud, it is possible for the hackers to corrupt an application and gain access to a mobile device while accessing

that application. In order to avoid these, strong virus-scanning and malware protection software need to be installed to avoid any type of virus/malware check into the mobile system. Besides, by embedding device identity protection, like allowing access to the authorized user based on some form of identity check feature and this will allow blocking unauthorized access.

Two types of services, have been defined in [1], namely (i) critical security service, and (ii) normal security service. The resource in a cloud has to be properly partitioned according to different user's requests. The maximal system rewards and system service overheads are considered for the security service. Hence, we see that although mobile cloud computing is still in its nascent state, there are various security issues, that haunt cloud computing and its derivatives.

3. THREATS TO SECURITY IN CLOUD COMPUTING

The chief concern in cloud environments is to provide security around multi-tenancy and isolation, giving customers more comfort besides "trust us" idea of clouds [45]. There has been survey works reported that classifies security threats in cloud based on the nature of the service delivery models of a cloud computing system [69]. However, security requires a holistic approach. Service delivery model is one of many aspects that need to be considered for a comprehensive survey on cloud security. Security at different levels such as Network level, Host level and Application level is necessary to keep the cloud up and running continuously. In accordance with these different levels, various types of security breaches may occur. These have been classified in rest of this section.

3.1. Basic Security

Web 2.0, a key technology towards enabling the use of Software as a Service (SaaS) relieves the users from tasks like maintenance and installation of software. It has been used widely all around. As the user community using Web 2.0 is increasing by leaps and bounds, the security has become more important than ever for such environment [67, 58, 48].

SQL injection attacks, are the one in which a malicious code is inserted into a standard SQL code and thus the attackers gain unauthorized access to a database and become able to access sensitive information. Sometimes the hacker's input data is misunderstood by the web-site as the user data and allows it to be accessed by the SQL server and this lets the attacker to have know-how of the functioning of the website and make changes into that. Various techniques like: avoiding the usage of dynamically generated SQL in the code, using filtering techniques to sanitize the user input etc to check the SQL injection attacks.

Cross Site Scripting (XSS) attacks, which inject malicious scripts into Web contents have become quite popular since the inception of Web 2.0. Based on the type of services provided, a website can be classified as static or dynamic. Static websites don't suffer from the security threats which the dynamic websites do because of their dynamism in providing multi-fold services to the users.

As a result, these dynamic websites get victimized by XSS attacks. It has been observed quite often that amidst working on net or surfing, some web-pages or pop-ups get opened up with the request of being clicked away to view the content contained in them. More often either unknowingly (about the possible hazards) or out of curiosity users click on these hazardous links and thus the intruding third party gets control over the user's private information or hack their accounts after having known the information available to them. Various techniques like: Active Content Filtering, Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology has already been proposed [30]. These technologies adopt various methodologies to detect security flaws and try to fix them.

Another class of attacks quite popular to SaaS are termed as Man in the Middle attacks (MITM). In such an attack, an intruder tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them. Various tools implementing strong encryption technologies like: Dsniff, Cain, Ettercap, Wsniff, Airjack etc have been developed in order to provide safeguard against them. A detailed study towards preventing man in the middle attacks has been presented in [29].

A few of the important points like: evaluating software as a service security, separate endpoint and server security processes, evaluating virtualization at the end-point have been mentioned by Eric Ogren, recently in an article at Security.com to tackle traditional security flaws [31].

Hence, security at different levels is necessary in order to ensure proper implementation of cloud computing such as: server access security, internet access security, database access security, data privacy security and program access security. In addition, we need to ensure data security at network layer, and data security at physical and application layer to maintain a secure cloud.

3.2. Network Level Security

Networks are classified into many types like: shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. To ensure network security following points such as: confidentiality and integrity in the network, proper access control and maintaining security against the external third party threats should be considered while providing network level security.

Problems associated with the network level security comprise of: DNS attacks, Sniffer attacks, issue of reused IP address, Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) etc.

- ***DNS attacks***

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems [26].

- ***SNIFFER attacks***

These types of attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [59].

- ***Issue of Reused Ip Addresses***

Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

- ***BGP prefix hijacking***

Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made and hence malicious parties get access to the untraceable IP addresses. On the internet, IP space is associated in blocks and remains under the control of AS's. An autonomous system can broadcast information of an IP contained in its regime to all its neighbours.

These ASs communicate using the Border Gateway Protocol (BGP) model. Sometimes, due to some

error, a faulty AS may broadcast wrongly about the IPs associated with it. In such case, the actual traffic gets routed to some IP other than the intended one. Hence, data is leaked or reaches to some other destination that it actually should not. An autonomous security system for autonomous systems has been explained in [37].

3.3. Application Level Security

Application level security refers to the usage of software and hardware resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. Now a days, attacks are launched, being disguised as a trusted user and the system considering them as a trusted user, allow full access to the attacking party and gets victimized. The reason behind this is that the outdated network level security policies allow only the authorized users to access the specific IP address. With the technological advancement, these security policies have become obsolete as there have been instances when the system's security has been breached, having accessed the system in the disguise of a trusted user. With the recent technological advancements, it's quite possible to imitate a trusted user and corrupt entire data without even being noticed.

Hence, it is necessary to install higher level of security checks to minimize these risks. The traditional methods to deal with increased security issues have been to develop a task oriented ASIC device which can handle a specific task providing greater levels of security with high performance [41]. But with application-level threats being dynamic and adaptable to the security checks in place, these closed systems have been observed to be slow in comparison to the open ended systems.

The capabilities of a closed system as well as the adaptability of an open ended system have been incorporated to develop the security platforms based on Check Point Open Performance Architecture using Quad Core Intel Xeon Processors [41]. Even in the virtual environment, companies like VMware etc are using Intel Virtualization technology for better performance and security base. It has been observed that more often websites are secured at the network level and have strong security measures but there may be security loopholes at the application level which may allow information access to unauthorized users. The threats to application level security include XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, DoS attacks, Backdoor and Debug Options, CAPTCHA Breaking etc resulting from the unauthorized usage of the applications.

- ***Security concerns with the hypervisor***

Cloud Computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time, providing the resources to each operating system such that they do not interfere with each.

As the number of operating systems running on a hardware unit increase, the security issues concerned with those that of new operating systems also need to be considered. Because multiple operating systems would be running on a single hardware platform, it is not possible to keep track of all and hence maintaining all the operating systems secure is difficult. It may happen that a guest system tries to run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest operating systems [33].

It cannot be denied that there are risks associated with sharing the same physical infrastructure between a set of multiple users, even one being malicious can cause threats to the others using the same infrastructure [35], and hence security with respect to hypervisor is of great concern as all the guest systems are controlled by it. If a hacker is able to get control over the hypervisor, he can make changes to any of the guest operating systems and get control over all the data passing through the hypervisor.

Various types of attacks can be launched by targeting different components of the hypervisor [51]. Based on the learning of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs and inter-communication among the various infrastructure components [36, 64].

□ ***Denial of service attacks***

A DoS attack is an attempt to make the services assigned to the authorized users unable to be used by them. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error. This happens when the number of requests that can be handled by a server exceeds its capacity. The occurrence of a DoS attack increases bandwidth consumption besides causing congestion, making certain parts of the clouds inaccessible to the users. Using an Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks [14]. A defence federation is used in [4] for guarding against such attacks. Each cloud is loaded with separate IDS. The different intrusion detection systems work on the basis of information exchange. In case a specific cloud is under attack, then the co-operative IDS alert the whole system. A decision on trustworthiness of a cloud is taken by voting, and the overall system performance is not hampered.

□ ***Cookie poisoning***

It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a web-page. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user. This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data [52].

□ ***Hidden field manipulation***

While accessing a web-page, there are certain fields that are hidden and contain the page related information and basically used by developers. However, these fields are highly prone to a hacker attack as they can be modified easily and posted on the web-page. This may result in severe security violations [53].

□ ***Backdoor and debug options***

A common habit of the developers is to enable the debug option while publishing a web-site. This enables them to make developmental changes in the code and get them implemented in the web-site. Since these debug options facilitate back-end entry to the developers, and sometimes these debug options are left enabled unnoticed, this may provide an easy entry to a hacker into the web-site and let him make changes at the web-site level [59].

□ ***Distributed denial of service attacks***

DDoS may be called an advanced version of DOS in terms of denying the important services running on a server by flooding the destination sever with an umpteen number of packets such that the target server is not able to handle it. In DDoS the attack is relayed from different dynamic networks which have already been compromised unlike DOS. The attackers have the power to control the flow of information by allowing some information available at certain times. Thus the amount and type of information available for public usage is clearly under the control of the attacker [2].

The DDoS attack is run by three functional units: A Master, A Slave and A Victim. Mater being the attack launcher is behind all these attacks causing DDoS, Slave is the network which acts like a launch pad for the Master. It provides the platform to the Master to launch the attack on the Victim. Hence it is also called as co-ordinated attack.

Basically a DDoS attack is operational in two stages: the first one being Intrusion phase where the Master tries to compromise less important machines to support in flooding the more important one. The next one is installing DDoS tools and attacking the victim server or machine. Hence, a DDoS attack results in making the service unavailable to the authorized user similar to the way it is done in a DoS attack but different in the way it is launched. A similar case of Distributed Denial of Service attack was experienced with CNN news channel website leaving most of its users unable to access the site for a period of three hours [50].

In general, the approaches used to fight the DDoS attack involve extensive modification of the underlying network. These modifications often become costly for the users. [2] proposed a swarm based logic for guarding against the DDoS attack. This logic provides a transparent transport layer,

through which the common protocols such as HTTP, SMTP, etc, can pass easily. The use of IDS in the virtual machine is proposed in [8] to protect the cloud from DDoS attacks. A SNORT like intrusion detection mechanism is loaded onto the virtual machine for sniffing all traffics, either incoming, or out-going. Another method commonly used to guard against DDoS is to have intrusion detection systems on all the physical machines which contain the user's virtual machines [16]. This scheme had been shown to perform reasonably well in a Eucalyptus [17] cloud.

- ***CAPTCHA breaking***

CAPTCHA's were developed in order to prevent the usage of internet resources by bots or computers. They are used to prevent spam and overexploitation of network resources by bots. Even the multiple web-site registrations, dictionary attacks etc by an automated program are prevented using a CAPTCHA.

But recently, it has been found that the spammers are able to break the CAPTCHA [14], provided by the Hotmail and G-mail service providers. They make use of the audio system able to read the CAPTCHA characters for the visually impaired users and use speech to text conversion software to defeat the test. In yet another instant of CAPTCHA Breaking it was found that the net users are provided some form of motivation towards solving these CAPTCHA's by the automated systems and thus CAPTCHA Breaking takes place.

- ***GOOGLE hacking***

Google has emerged as the best option for finding details regarding anything on the net. Google hacking refers to using Google search engine to find sensitive information that a hacker can use to his benefit while hacking a user's account. Generally, hackers try to find out the security loopholes by probing out on Google about the system they wish to hack and then after having gathered the necessary information, they carry out the hacking of the concerned system. In some cases, a hacker is not sure of the target. Instead he tries to Google out the target based on the loophole he wishes to hack a system upon. The hacker then searches all the possible systems with such a loophole and finds out those having the loopholes he wishes to hack upon. A Google hacking event was observed recently when login details of various g-mail users were stolen by a group of hackers in China. These had been some of the security threats that can be launched at the application level and cause a system downtime disabling the application access even to the authorized users.

- ***Some general points on cloud security***

Neural Net Algorithms has a big part in Intrusion Detection system. [72] describes a novel way of Neural Net algorithms. [73] and [74] describes two other algorithms on Intrusion Detection Systems. Data travelling between Cloud and Point of action does go through areas, vulnerable to virus attacks. [75] provides a novel way of Data Transfer in such cases, offering possible minimization of data destruction.

4. DATA STORAGE AND SECURITY

Many cloud service providers provide storage as a form of service. They take the data from the users and store them on large data centres, hence providing users a means of storage. Although these cloud service providers say that the data stored in the cloud is utmost safe but there have been cases when the data stored in these clouds have been modified or lost may be due to some security breach or some human error.

Various cloud service providers adopt different technologies to safeguard the data stored in their cloud. But the question is: Whether the data stored in these clouds is secure enough against any sort of security breach? The virtualized nature of cloud storage makes the traditional mechanisms unsuitable for handling the security issues. These service providers use different encryption techniques like public key encryption and private key encryption to secure the data resting in the cloud. A similar technique providing data storage security, utilizing the homo-morphic token with distributed verification of erasure-coded data has been discussed in [21]. Trust based methods are useful in establishing relationships in a distributed environment. A domain based trust-model has been proposed in [7] to handle security and interoperability in cross clouds. Every domain has a special agent for trust management. It proposes

different trust mechanisms for users and service providers.

Another major issue that is mostly neglected is of Data-Remanence. It refers to the data left out in case of data transfer or data removal. It causes minimal security threats in private cloud computing offerings, however severe security issues may emerge out in case of public cloud offerings as a result of data-remanence [42].

Various cases of cloud security breach came into light in the last few months. Cloud based email marketing services company, Epsilon suffered the data breach, due to which a large section of its customers including JP Morgan Chase, Citibank, Barclays Bank, hotel chains such as Marriott and Hilton, and big retailers such as Best Buy and Walgreens were affected heavily and huge chunk of customer data was exposed to the hackers which includes customer email ids and bank account details.

Another similar incident happened with Amazon causing the disruption of its EC2 service [15, 20]. The damage caused had proved to be quite costly for both the users and the system administrators [18]. Popular sites like: Quora, Four-Square and Reditt were the main sufferers [57]. The above mentioned events depict the vulnerability of the cloud services.

Another important aspect is that the known and popular domains have been used to launch malicious software or hack into the companies' secured database. A similar issue happened with Amazon's S3 platform and the hackers were able to launch corrupted codes using a trusted domain [49] and hence the question that arises now is who to be provided the "trusted" tag. It proved that Amazon is prone to side-channel attacks, and a malicious virtual machine, occupying the same server as the target, can easily gain access to confidential data [12]. The question is: whether any such security policy should be in place for these trusted users as well?

An incident relating to the data loss occurred last year with the online storage service provider "Media max" also known as "The Linkup" when due to system administration error, active customer data was deleted, leading to the data loss. SLA's with the Cloud Service providers should contain all the points that may cause data loss either due to some human or system generated error. Hence, it must be ensured that redundant copies of the user data should be stored in order to handle any sort of adverse situation leading to data loss.

Virtualization in general increases the security of a cloud environment. With virtualization, a single machine can be divided into many virtual machines, thus providing better data isolation and safety against denial of service attacks [10]. The VMs provide a security test-bed for execution of untested code from un-trusted users. A hierarchical reputation system has been proposed in the paper [10] for managing trust in a cloud environment.

5. ENSURING SECURITY AGAINST THE VARIOUS TYPES OF ATTACKS

In order to secure the cloud against the various security threats and attacks like: SQL injection, Cross Site Scripting (XSS) attacks, DoS and DDoS attacks, Google Hacking and Forced Hacking, different cloud service providers adopt different techniques. A few standard techniques in order to detect the above mentioned attacks are as: Avoiding the usage of dynamically generated SQL in the code, finding the meta-structures used in the code, validating all user entered parameters, disallowing and removal of unwanted data and characters, etc. A generic security framework needs to be worked out for an optimized cost performance ratio. The main criterion to be filled up by the generic security framework are to interface with any type of cloud environment, and to be able to handle and detect predefined as well as customized security policies.

A similar approach is being used by Symantec Message Labs Web Security cloud that blocks the security threats originating from internet and filters the data before they reach the network. Web security cloud's security architecture rests on two components:

a. *Multi layer security: In order to ensure that data security and block possible malwares, it consists of multi-layer security and hence a strong security platform.*
b. *URL filtering: It is being observed that the attacks are launched through various web*

pages and internet sites and hence filtering of the web-pages, ensures that no such harmful or threat carrying web page gets accessible. Also, content from undesirable sites can be blocked.

With its adaptable technology, it provides security even in highly conflicting environments and ensures protection against new and converging malware threats.

A Google hacking database identifies the various types of information such as: login passwords, pages containing logon portals, session usage information etc. Various software solutions such as Web Vulnerability Scanner can be used to detect the possibility of a Google hack. In order to prevent Google hack, the user needs to ensure that only those information that does not affect him should be shared with the Google. This would prevent sharing of any sensitive information that may result in adverse conditions.

The symptoms to a DoS or DDoS attack are: system speed gets reduced and programs run very slowly, large number of connection requests from a large number of users, less number of available resources. Although when launched in full strength DDoS attacks are very harmful as they exhaust all the network resources, still a careful monitoring of the network can help in keeping these attacks in control.

In case of IP spoofing an attacker tries to spoof the users that the packets are coming from reliable sources. Thus the attacker takes control over the client's data or system showing himself as the trusted party. Spoofing attacks can be checked by using encryption techniques and performing user authentication based on Key exchange. Techniques like IPSec do help in mitigating the risks of spoofing. By enabling encryption sessions and performing filtering at the incoming and outgoing entrances spoofing attacks can be reduced.

Every cloud service provider has installed various security measures depending on its cloud offering and the architecture. Their security model largely depends upon the customer section being served, type of cloud offering they provide and the deployment models they basically implement as discussed in [68].

Table 1. Comparative Analysis for Strengths and Limitations of Some of the Existing Security Schemes

Security Scheme	Suggested Approach	Strengths	Limitations
Data Storage security [21]	Uses homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security and locating the server being attacked.	1. Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data modification and server colluding attacks as well as against byzantine failures.	The security in case of dynamic data storage has been considered. However, the issues with fine-grained data error location remain to be addressed.
User identity safety in cloud computing	Uses active bundles scheme, whereby predicates are compared over encrypted data and multiparty computing.	Does not need trusted third party (TTP) for the verification or approval of user identity. Thus the user's identity is not disclosed. The TTP remains free and could be used for other purposes such as decryption.	Active bundle may not be executed at all at the host of the requested service. It would leave the system vulnerable. The identity remains a secret and the user is not granted permission to his requests.
Trust model for interoperability and security in cross cloud [35]	1. Separate domains for providers and users, each with a special trust agent. 2. Different trust strategies for service providers and customers. 3. Time and transaction factors are taken into account for trust assignment.	1. Helps the customers to avoid malicious suppliers. 2. Helps the providers to avoid co-operating/serving malicious users.	Security in a very large scale cross cloud environment. This scheme is able to handle only a limited number of security threats in a fairly small environment.
Virtualized defence and reputation based trust management	1. Uses a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. 2. Lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks.	Extensive use of virtualization for securing clouds	The proposed model is in its early developmental stage and needs further simulations to verify the performance.

Security Scheme	Suggested Approach	Strengths	Limitations
Secure virtualization [61]	1. Idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware is proposed. 2. Behaviour of cloud components can be monitored by logging and periodic checking of executable system files.	A virtualized network is prone to different types of security attacks that can be launched by a guest VM, an ACPS system monitors the guest VM without being noticed and hence any suspicious activity can be blocked and system's security system notified.	System performance gets marginally degraded and a small performance penalty is encountered. This acts as a limitation towards the acceptance of an ACPS system.
Safe, virtual network in cloud environment [35]	Cloud Providers have been suggested to obscure the internal structure of their services and placement policy in the cloud and also to focus on side-channel risks in order to reduce the chances of information leakage.	Ensures the identification of adversary or the attacking party and helping us find a far off place for an attacking party from its target and hence ensuring a more secure environment for the other VMs.	If the adversary gets to know the location of the other VMs, it may try to attack them. This may harm the other VMs in between.
Border Gateway Protocol (BGP) [37]	A pretty good BGP (PGBGP) architecture has been suggested to check the cases where an Autonomous system may announce itself wrongly as the destination for all the data that is being transferred over that network..	Checks the autonomous systems (ASs) and performs anomaly detection with a response system to ensure that the data doesn't get routed to the wrong AS. It also gives us the flexibility to run the PGBGP protocol on some of the ASs towards protecting the entire network.	Vulnerable to Denial of Service (DoS) attacks. This approach only takes care of the routing control messages but doesn't verify the path that actual traffic follows.

One of the security measures implemented by SalesForce.com to avoid unauthorized access to its platform is sending a security code to the registered customer every-time, the same account is accessed from a different IP-address and the user needs to provide the security code at the time of logging in, in order to prove its identity [56].

It is equally important to secure the data in transit and security of transmitted data can be achieved through various encryption and decryption schemes. In such a scenario, even if the data gets into the hands of a hacker, he won't be able to make any unauthorized use until he knows how to decrypt it. A few of the encryption-decryption techniques include private and public key encryption. In a symmetric key (private key) encryption such as: DES, Triple DES, RC2, RC4 etc, the same key is used for encryption and decryption. Before the data is transferred, the key is shared between both the receiver and the sender. Sender then sends the data after having encrypted it using the key and the receiver decrypts it using the same key.

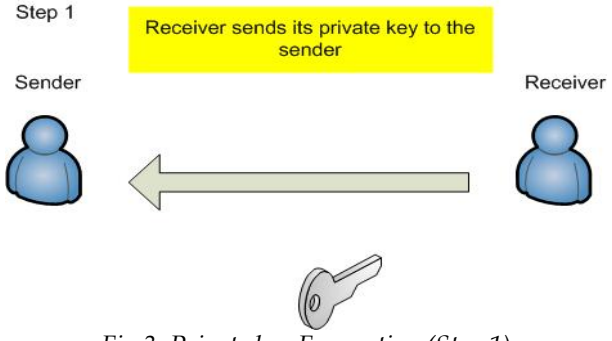

Fig 3. Private key Encryption (Step 1)

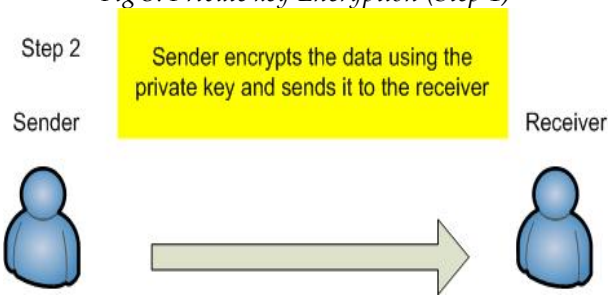

Fig 4. Private Key encryption (Step 2)

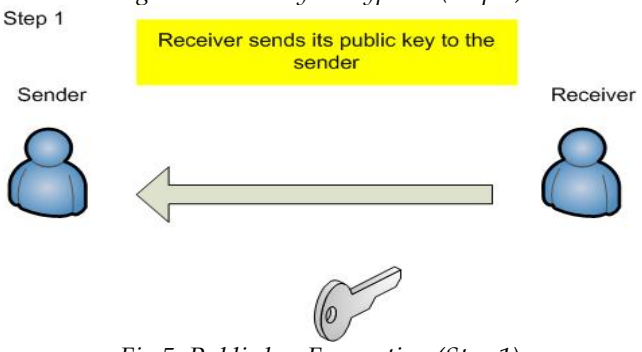

Fig 5. Public key Encryption (Step 1)

In case of an asymmetric key algorithm (RSA, DSA, PGP etc), there are two sets of keys known as public key and private key. The keys occur in pairs which means that a specific public key can only be decrypted using the private key linked to it. In such an encryption technique the sender encrypts the data using the public key and then sends it to the receiver which at the receiving end

makes use of corresponding private key to decrypt the same.

Hence, we can see that although Public key encryption may take a bit more processing time in comparison to the private key encryption, but in cases where security is more of a concern rather than the speed, public-key encryption provides more secure data transmission in comparison to private-key encryption. Security issues in a virtualized environment wherein a malicious virtual machine tries to take control of the hypervisor and access the data belonging to other VMs have been observed and since traffic passing between VMs doesn't travel out into the rest of the data-centre network and hence cannot be seen by regular network based security platforms [46].

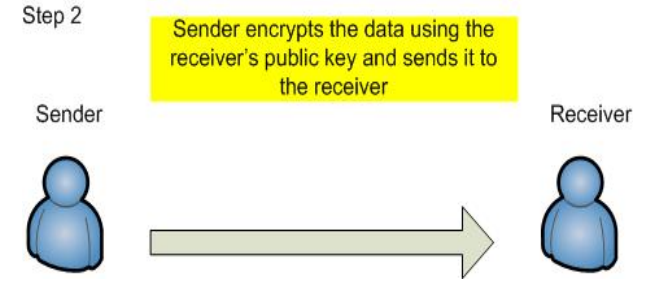

Fig 6. Public key Encryption (Step 2)

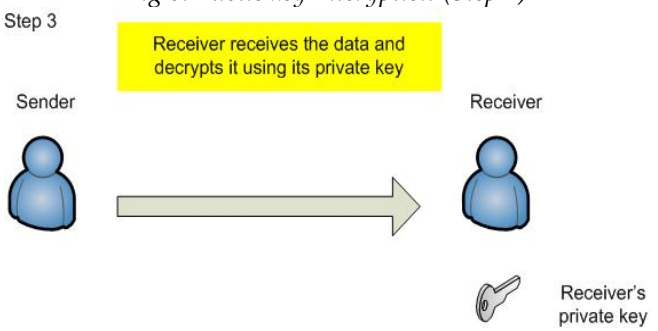

Fig 7. Public key Encryption (Step 3)

Hence, there is a need to ensure that security against the virtual threats should also be maintained by adopting the methodologies such as: keeping in check the virtual machines connected to the host system and constantly monitoring their activity, securing the host computers to avoid tampering or file modification when the virtual machines are offline, preventing attacks directed towards taking control of the host system or other virtual machines on the network etc.

A security model wherein a dedicated monitoring system taking care of the data coming in and out of a virtual machine/machines functional in a virtualized environment on a hypervisor can be presented as shown below:

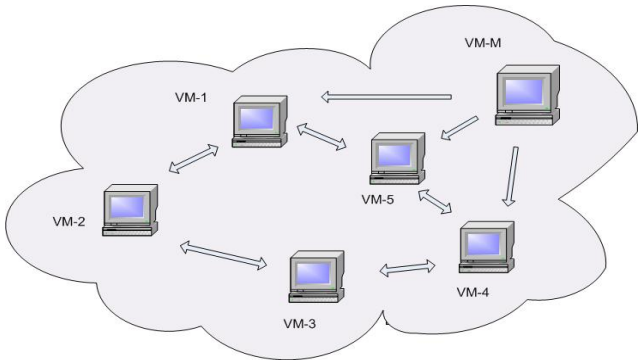

Fig. 8 Security Model in a Virtualized Environment

As can be seen from the above shown security model, a Virtual machine monitor can be placed in a virtual environment which will keep track of all the traffic flowing in and out of a virtual machine network. And in case if there is any suspicious activity observed, the corresponding virtual machine may be de-linked or blocked and hence maintaining the security of the virtualized network.

The security breach of Twitter and Vaserv.com (via a zero-day vulnerability) last year and the data breach at Sony Corporation and Go-Grid [47], this year, compromising 100 million customers' [38], data have made it quite clear that stringent security measures are needed to be taken in order to ensure security and proper data control in the cloud.

Thus we see that the security model adopted by a Cloud service provider should safeguard the cloud against all the possible threats and ensure that the data residing in the cloud doesn't get lost due to some unauthorized control over the network by some third party intruder.

6. CONCLUSION

Cloud Computing, envisioned as the next generation architecture of IT Enterprise is a talk of the town these days. Although it has revolutionized the computing world, it is prone to manifold security threats varying from network level threats to application level threats. In order to keep the Cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. Auditing of the cloud at regular intervals needs to be done to safeguard the cloud against external threats. In

addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. In this paper various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed.

REFERENCES

[1]. *H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource allocation for security services in mobile cloud computing," in Proc. IEEE INFOCOM'11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, April 10-15, 2011, Shanghai, China.*

[2]. *Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.*

[3]. *Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, "SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment," Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, Yantai, Shandong, China, 2010. ISBN: 978-1-4244-5958-2.*

[4]. *Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.*

[5]. *Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.*

[6]. *Michael Kretzschmar, S Hanigk, "Security management interoperability challenges for collaborative clouds," Systems and Virtualization Management (SVM), 2010, Proceedings of the 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and the Cloud, pp. 43-49, October 25-29, 2010. ISBN: 978-1-4244-9181-0, DOI: 10.1109/SVM.2010.5674744.*

[7]. *W. Li, L. Ping, X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," 2010 International Conference on Electronics and Information Engineering (ICEIE), Volume: 1, pp. V1-14 - V1-19, 2010. DOI: 10.1109/ICEIE.2010.5559829.*

[8]. *Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.*

[9]. *B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.*

[10]. *K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695-3929-4. DOI: http://doi.ieeecomputersociety.org/10.1109/DASC.2009.149.*

[11]. *R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing," The World Privacy Forum, 2009. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.*

[12]. *Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, "Hey, you get off my cloud: Exploring information leakage in third party compute clouds," CCS'09, Proceedings of the 16th ACM conference. On Computer and Communications Security, pp. 199-212, ACM New York, NY, USA, 2009. ISBN: 978-1-60558-894-0.*

[13]. *L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009. DOI: 10.1109/ICWS.2009.144.*

[14]. *K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010. DOI: 10.1109/MITP.2009.89.*

[15]. *"Amazon ec2 sip brute force attacks on rise", http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/.*

[16]. *Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," Sixth International Conference on Information Assurance and Security, USA, pp. 265-270, Aug. 23-25, 2010. DOI: 10.1109/ISIAS.2010.5604069.*

[17]. *"Eucalyptus web site," http:// www.eucalyptus.com/. [Eucalyptus is the world's most widely deployed software platform for on-premise (private) Infrastructure-as-a-Service (IaaS) clouds. To date, over 25,000 Eucalyptus clouds have been started up all over the globe including more than 2 out of every 5 Fortune 100 companies.]*

[18]. *D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus open-source cloud-computing system," in Proceedings of the 9th IEEE/ACM International*

Symposium on Cluster Computing and the Grid (CCGRID '09), pp. 124–131, 2009.

[19]. *"Sip attacks from Amazon ec2 cloud continue," http://www.voiptechchat.com/voip/538/sip-attacks-from- amazon-ec2-cloud-continue /.*

[20]. *"EC2 web site," http://aws.amazon.com/ec2/. [From Amazon EC2's web site: "Amazon Elastic Compute Cloud (Amazon EC2)".]*

[21]. *Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service,2009, IWQoS, Charleston, SC, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4*

[22]. *Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.*

[23]. *R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.*

[24]. *S. Pearson, "Taking account of privacy when designing cloud computing services," CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE Computer Society Washington, DC, USA, May 2009. ISBN: 978-1-4244-3713-9.*

[25]. *Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.*

[26]. *Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats," http://searchsecurity.techtarget.com/tip/0, 289483, sid14_gci1359155_mem1, 00.html/.*

[27]. *Lori M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009, ISSN: 1540-7993, INSPEC Accession Number: 10805344, DOI: 10.1109/MSP.2009.87.*

[28]. *Neal Leavitt, "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, issue. 1, pp. 15-20, IEEE Computer Society, CA, USA, January 2009. ISSN: 0018-9162.*

[29]. *Jonathan Katz, "Efficient Cryptographic Protocols Preventing Man in the Middle Attacks," Doctoral Dissertation submitted at Columbia University, 2002, ISBN: 0-493-50927-5. http://www.cs.ucla.edu/~rafail/STUDENTS/katz-thesis.pdf /.*

[30]. *Web 2.0/SaaS Security, Tokyo Research Laboratory, IBM Research. http://www.trl.ibm.com/projects/web20sec/web20sec_e.htm.*

[31]. *Eric Ogren, "Whitelists SaaS modify traditional security, tackle flaws," Sep. 17, 2009. http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1368647,00.html/.*

[32]. *Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, "Automated Control in Cloud Computing: Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.*

[33]. *Daniel Petri, "What You Need to Know About Securing Your Virtual Network," Jan. 8, 2009. http://www.petri.co.il/what-you-need-to-know-about-vmware-virtualization-security.htm/.*

[34]. *John E. Dunn, "Spammers break Hotmail's CAPTCHA yet again", Tech-world, 16th Feb. 2009. http://news.techworld.com/security/110908/spammers-break-hotmails-captcha-yet-again/.*

[35]. *Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security," Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.*

[36]. *Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing," Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.*

[37]. *Josh Karlin, Stephanie Forrest, Jennifer Rexford, "Autonomous Security for Autonomous Systems," Proc. of Complex Computer and Communication Networks; vol. 52, issue. 15, pp. 2908- 2923, Oct. 2008, Elsevier North-Holland, Inc. New York, NY, USA.*

[38]. *Czaroma Roman, "Sony Data Breach Highlights Importance of Cloud Security," Cloud Times, May 9, 2011. http://cloudtimes.org/sony-data-breach-highlights-importance-of-cloud-security/.*

[39]. *Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009; ISBN: 978-0596802769. http://oreilly.com/catalog/9780596802776.*

[40]. *Hamid R. Motahari-Nezhad, Claudio Bartolini, Sven Graupner, Sharad Singhal, Susan Spence, "IT Support Conversation Manager: A Conversation-Centered Approach and Tool for Managing Best Practice IT Processes," Proceedings of the 2010 14th IEEE International Enterprise Distributed Object Computing Conference, pp. 247-256, October 25-29, 2010, ISBN: 978-1-4244-7966-5.*

[41]. *Scalable Security Solutions, Check Point Open Performance Architecture, Quad-Core Intel Xeon*

Processors, "Delivering Application-Level Security at Data Centre Performance Levels," Intel Corporation, 2008. http://download.intel.com/netcomms/technologies/security/320923.pdf.

[42]. Jason Bloomberg, "Data Remanence: Cloud Computing Shell Game," May 19, 2011. http://www.zapthink.com/2011/05/19/data-remanence-cloud-computing-shell-game/.

[43]. Olafur Ingthorsson; "Improving the Mobile Cloud", July 18, 2011 in Cloud Computing and Mobile Cloud Computing. http://cloudcomputingtopics.com/2011/07/improving-the-mobile-cloud/.

[44]. Jessica T., "Connecting Data Centres over Public Networks," IPEXPO.ONLINE, April 20, 2011. http://online.ipexpo.co.uk/2011/04/20/connecting-data-centres-over-public-networks/.

[45]. "Security Consideration for Cloud Ready Data-Centres," Juniper Networks, Oct. 2009. http://www.juniper.net/us/en/local/pdf/whitepapers/2000332-en.pdf.

[46]. Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessicca Staddon, Ryusuke Masuoka, Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," Proc. of the ACM Workshop on Cloud Computing Security, pp. 85-90, USA, November, 2009. ISBN: 978-1-60558-784-4.

[47]. Go-Grid Security Breach, April, 2011. http://doj.nh.gov/consumer/security breaches/documents/gogrid-20110401.pdf [Letters to customers and parties involved, informing them about the Go-Grid security breach].

[48]. Adam A Noureddine, Meledath Damodaran, "Security in Web 2.0 Application Development," iiWAS '08, Proc. of the 10th International Conference on Information Integration and Web-based Applications & Services, pp. 681-685, 2008, ISBN: 978-1-60558-349-5, DOI: 10.1145/1497308.1497443.

[49]. Rory Smith, "The Use of Legitimate Channels to distribute malicious software to Users. http://www.thesecuritysamurai.com/2011/08/02/the-use-of-legitimate-channels-to-distribute-malicious-software-to-users-by-rory-smith-soc-analyst/.

[50]. Nathan Mcfeters, "Recent CNN Distributed Denial of Service Attack Explained". http://www.zdnet.com/blog/security/recent-cnn-distributed-denial-of-service-ddos-attack-explained/1054.

[51]. Berman, M., "Virtualization Audit 101: The top 5 risks and recommendations for protecting your virtual IT," Computer Technology Review, Feb. 4, 2009.http://www.wwpi.com/.

[52]. D. Gollmann, "Securing Web Applications," Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK, DOI: 10.1016/j.istr.2008.02.002.

[53]. Ian Rathie, "An Approach to Application Security," White Paper, SANS Institute. http://www.sans.org/reading_room/whitepapers/application/approach-application-security_16.

[54]. Julisch, K., & Hall, M., "Security and control in the cloud," Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.

[55]. Timothy Wood, Prashant Shenoy, Alexandre Gerber, K.K. Ramskrishnan, Jacobus Van der Merwe, "The Case for Enterprise-Ready Virtual Private Clouds," HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, CA, USA, 2009. http://www.usenix.org/event/hotcloud09/tech/full_papers/wood.pdf.

[56]. Security and Privacy policies of Sales-Force.com. http://trust.salesforce.com/trust/security/best_practices/ http://trust.salesforce.com/trust/privacy/tools/.

[57]. Amazon EC2 goes down, taking with it Reditt, FourSquare and Quora. http://eu.techcrunch.com/2011/04/21/amazon-ec2-goes-down-taking-with-it-reddit-foursquare-and-quora/.

[58]. Mashups, SaaS and Cloud Computing: Evolutions and Revolutions in the Integration Landscape. http://www.redcad.org/summerschool09/slides/Bentallah_CTDS09_Mashups%20and%20SaaS.pdf.

[59]. Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004, ISBN: 0-7695-2068-5.

[60]. Robert Minnear, "Latency: The Achilles Heel of Cloud Computing," March 9, 2011, Cloud Expo: Article, Cloud Computing Journal. http://cloudcomputing.sys-con.com/node/1745523.

[61]. Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing," Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

[62]. "Database Security in Virtualization and Cloud Computing Environment: The three key technology challenges in protecting sensitive data in modern IT architectures," Whitepaper, McAfee. https://portal.mcafee.com/downloads/General%20Documents/database_security_in_virtualization_and_cloud_computing_environments.pdf.

[63]. Jon Marler, "Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud," Rackspace Knowledge Centre, March 27, 2011, Article Id: 1638. http://www.rackspace.com/knowledge_center/private-cloud/securing-the-cloud-addressing-cloud-computing-security-concerns-with-private-cloud.

[64]. Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and

Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[65]. George V. Hulme, "NIST formalizes cloud computing definition, issues security and privacy guidance," Feb. 3, 2011 [A common platform enabling security executives to share best security practices and strategic insights]. http://www.csoonline.com/article/661620/nist-formalizes-cloud-computing-definition-issues-security-and-privacy-guidance.

[66]. "Security Considerations White Paper for Cisco Smart Storage," Cisco Systems, 2010. http://www.cisco.com/en/US/docs/storage/nass/csbcdp/smart_storage/white_paper/Security_Considerations_OL-23025.pdf.

[67]. Pradnyesh Rane, "Securing SaaS Applications: A Cloud Security Perspective for Application Providers," Information Systems Security, 2010. http://www.infosectoday.com/Articles/Securing_SaaS_Applications.htm.

[68]. Amitav Chakravartty, Serena Software, "Serena Service Manager Security in the Cloud". http://www.serena.com/docs/repository/products/service-manager/Serena-Service-Manager-Security-in-the-Cloud.pdf.

[69]. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.

[70]. R. L. Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, Mar-April, 2009, ISSN: 1520-9202, INSPEC Accession Number: 10518970, DOI: 10.1109/MITP.2009.40.

[71]. Frederik De Keukelaere, Sumeer Bhola, Michael Steiner, Suresh Chari, Sachiko Yoshihama, "Smash: secure component model for cross-domain mashups on unmodified browsers," Proc. of the 17th International Conference on World Wide Web, ACM, NY, USA, 2008, ISBN: 978-1-60558-085-2, DOI: 10.1145/1367497.1367570.

[72]. Zhihua Cui, Chunxia Yang, Sugata Sanyal; "Training Artificial Neural Networks using APPM"; International Journal of Wireless and Mobile Computing; Editor-in-Chief: Zhihua Cui; Vol.5, Nos. 2,2012, pp.168-174. ISSN (Online): 1741-1092; ISSN (Print): 1741-1084.DOI: 10.1504/IJWMC.2012.046787

[73]. Animesh Kr Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal and Sugata Sanyal, RISM - Reputation Based Intrusion Detection System for Mobile Ad hoc Networks, Third International Conference on Computers and Devices for Communications, CODEC-06, pp. 234-237. Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006, Kolkata, India

[74]. Ajith Abraham, Ravi Jain, Sugata Sanyal and Sang Yong Han, SCIDS: A Soft Computing Intrusion Detection System, 6th International Workshop on Distributed Computing (IWDC-2004), A. Sen et al (Eds.), Springer Verlag, Germany, Lecture Notes in Computer Science, Vol. 3326, ISBN: 3-540-24076-4, pp. 252-257, 2004.

[75]. RA Vasudevan, A Abraham, S Sanyal, DP Agrawal, Jigsaw Based Secure Data Transfer over Computer Networks, Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004

[76]. Sandipan Dey, Ajith Abraham and Sugata Sanyal "An LSB Data Hiding Technique Using Natural Numbers", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2007, Nov 26-28, 2007, Kaohsiung City, Taiwan, IEEE Computer Society press, USA, ISBN 0-7695-2994-1, pp. 473-476, 2007

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING
ISSN:2067-3809

copyright ©
University "POLITEHNICA" Timisoara,
Faculty of Engineering Hunedoara,
5, Revolutiei,
331128, Hunedoara, ROMANIA
http://acta.fih.upt.ro