Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Security Issues In Cloud Computing

R.Usha[1], R. Sharmily[2]
[1,2]*Department of computer science and engineering*
*Velammal Institute of Technology, Chennai, India*

***Abstract--Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources. In our paper we have discussed However, security and privacy concerns are shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the security community. Addressing these challenges requires, in addition to the ability to cultivate and tune the security measures developed for traditional computing systems, proposing new security policies, models, and protocols to address the unique cloud security challenges. In this work, we provide a comprehensive study of cloud computing security and privacy concerns. We investigate and identify the limitations of the current solutions and provide insights of the future security perspectives.***

## I. CLOUD COMPUTING

Cloud computing is a way of providing IT services over the internet. A cloud computing services provider can offer huge amounts of data storage space and complete business applications to multiple customers to use on demand.The economies of scale achieved by providing cloud services to multiple customers at the same time allows the provider to offer his/her services cheaper than customers could organise for themselves. Furthermore, cloud computing offers customers easy access and immediate availability to respond to their needs and they do not need to devote any extra floor space to house the service because the service is delivered remotely.

## II. BENEFITS

Through cloud computing, businesses, consumers or public organizations can use services that they would not otherwise be able to afford. In particular, small organizations or individuals are able to use highly advanced services that could, in turn, allow them to develop and sell their own services. Cloud computing, therefore, offers an enormous potential for creativity and innovation in the services available on the internet.

Some examples of its use:

Social networking sites may offer their members, irrespective of their technical skills, the opportunity to develop games, birthday calendars and so on, which the member can then advertise and sell on the site to other members. Sharing pictures on social networks is already common place.

Online customer relationship management: companies can manage their interactions with customers and potential clients, for instance, marketing or technical support of customers. These can be outsourced to large specialized organisations, sometimes based in other countries. As they only charge for the time and space actually used, even very small companies can afford highly developed services without having to buy and install specific software. The savings can then be used to improve the business in other ways.

Any software developer can use cloud computing services to rent the necessary development tools in order to create his or her own software products. As the developer only needs to pay for the services used for the amount of time they were used for, this offers significant savings compared to buying expensive software tool licenses for a period of time that exceeds what is needed.

### *A. Protection*

In many simple transactions between organizations providing a service and their customers, the data protection legal obligations and responsibilities for each party are easy to establish. The customer (data controller) determines the purposes and means of the processing of personal information, while the service provider (data processor) only acts upon instructions from the customer. The roles of each party are not as straightforward in cloud computing, where the cloud service provider often makes important decisions about the means and conditions of processing personal information, such as where the information is stored, the use of sub-contractors and security. In cloud computing, control over personal information is often shared between the customer and the

service provider. This is a fundamental departure from the traditional case where there is a clear distinction between the customer as controller and the service provider as processor.

If the division of obligations and responsibilities between cloud customers and cloud service providers does not reflect their actual role in the cloud computing service, there is a high risk that no one takes full responsibility for data protection obligations laid down in law. This might mean that insufficient protection is provided in practice.

Potential customers of cloud computing should be sure they fully understand the data protection consequences of any contract they enter into. Providers of cloud computing services should be willing to clearly explain and discuss the terms and conditions of providing their services - customers should beware if this is not the case. Providers of cloud computing services to the general public should also be aware of their responsibilities and ensure that customers fully understand the implications of contracts to help them make informed decisions to use these services.
Cloud computing architecture consists of three layers: (i) Software as a service (SaaS); (ii) Platform as a service (PaaS) and (iii) Infrastructure as a service (IaaS). The clouds are also viewed as five component architectures that comprise clients, applications, platforms, infrastructure and servers. The current clouds are deployed in one of four deployment models: (a) public clouds in which the physical infrastructure is owned and managed by the service provider; (b) community clouds in which the physical infrastructure is owned and managed by a consortium of organizations; (c) private clouds in which the infrastructure
is owned and managed by a specific organization and (d) hybrid clouds which include combinations of the previous three models

*B. Cloud Security Categories, Issues And Dependencies*

As part of this work, we have conducted a survey on the current cloud security issues and the state of- the-art security solutions. We have also provided a comparative analysis of the current security solutions and the state-of-the-art countermeasures.

We classify cloud computing security related issues into the following five categories

The Security Standards category deals with regulatory authorities and governing bodies that Define cloud security policies to ensure secure working environment over the clouds. It includes Service level agreements, auditing and other agreements among users, service provider and Other stakeholders.
The Network category refers to the medium through which the users connect to cloud Infrastructure to perform the desired computations. It includes browsers, network connections And information exchange through registration.
The Access Control category is a user-oriented category and includes identification, Authentication and authorization issues.
The Cloud Infrastructure category includes security issues within SaaS, PaaS and IaaS and is Particularly related with virtualization environment.

The Data category covers data integrity and confidentiality issues.

The first point belongs to Security Standards. That is it describes about the standards required to take precaution measures in cloud computing in order to prevent attacks. It governs the policies of cloud Computing for security without compromising reliability and performance.
The second is Network category which Involves network attacks such as Connection Availability, Denial of Service (DoS), DDoS, flooding attack, internet protocol vulnerabilities, *etc*
Third category is Access Control that Covers authentication and access control. It captures issues that affect privacy of user information and data storage.
Fourth deals with the cloud infrastructure that Covers attacks that are specific to the cloud infrastructure (IaaS, PaaS and SaaS) such tampered binaries and privileged insiders.
Finally it is the DataCovers data related security issues including data migration, integrity, Confidentiality, and data warehousing.

Currently, cloud computing lacks appropriate security standards. Even if security standards are defined properly, many security issues are still Associated with compliance risks due to lack of governess for audits and assessment of corporate standards. Cloud

customers do not have enough knowledge of procedures, processes and practices of the provider, especially in the areas of identity management and segregation of duties. Organizations that seek to obtain certifications may be put on risk by denying an audit by cloud customers. One of the most important aspect of cloud computing security is auditability; however, we do not have an audit net for cloud service providers. If a service provider outsources a service to a third party where functionality is not transparent, users must be able to inspect the whole process. Security standards and governing bodies are part of service level agreements (SLA) and legal aspects, respectively which have not been taken into practices for cloud computing. SLA defines the relationship among parties (provider—recipient) and is extremely important for both parties [9]. It includes identifying/defining the customer's needs, simplifying complex issues, encouraging dialog in the event of disputes, providing a framework for understanding, reducing/removing areas of conflict, eliminating unrealistic expectations. The user may suffer, in case of data loss, if the above factors are not taken into consideration as he may not be able to put claims on service providers. These interactions shape the Trust relationship between the users and the different cloud stakeholders which is required when users transfer data on cloud infrastructure Strong justifications are required to gain customers' trust in that regard. Hackers can occupy resources (hardware/application) by generating bogus data or they can run malicious code on the hijacked resources. Denial of service can be launched by first identifying vulnerabilities in Internet protocols such as SIP (Session Initiation Protocol) which could deem the Internet to be un-trusted.

### *C. Solutions Provided*

These applications are different in nature, based on different requirements, and there is no single hard and fast rule to implement the security measurements at the interface level. The solution provided in this article consists of the following modules:

*1) Sensor:* It monitors the incoming request messages. If it identifies that there is hypothetical increase in number of messages coming from same or particular consumer, it marks it as suspicious.

*2) HOP Count filter:* It will count the hop count value (how many nodes, does message traverse from source to destination) and compare it with pre-defined HOP count. If a difference is found, it means that the header or the message has been modified on hacker machine and thus is marked suspicious.

*3) IP Frequency Divergence:* Marks a message suspicious, if there is same frequency of IP messages.

*4) Double Signature:* It doubles the XML signature: one in header and one in bottom. In case of attack, both XML signatures need to be verified.

*5) Puzzle Solver:* It deals with some intelligent puzzles, where results should be imbedded in some Simple Object Access Protocol (SOAP) header. In case of attack (HTTP DDoS), the cloud defender will send back the puzzle to IP, from which it is receiving messages. If the cloud defender received back the solved puzzle then the request is deemed legitimate, otherwise it is marked as HTTP DDoS attack.

The problem in this framework is that it lacks practical validation and is based on the assumption that the number of modules in the system is directly proportional to the number of attacks expected. Moreover, exhaustive monitoring of messages on each node would considerably slow the network traffic. Finally, the framework lacks the proper mechanisms for node coordination in case of attack incidence detection. From the references made there is no strong solution available to prevent the DDoS attacks". To validate the claim, the authors conduct the experiment to evaluate the effectiveness of the actual security solutions against distributed attacks. The security solutions involved in the experiment are SNORT and commercial firewall. The authors conclude that the failure of security systems lies within two aspects: either the security solution can be obsolete because it is not updated, or the solution can rely on unsuitable methods. They did not propose any solution that can prevent distributed security attacks. Other widely used DDoS countermeasures are firewalls. However, due to firewall location (at the border of a network), it would not be able to detect distributed attacks once they are in the network.

### *D. Malware Injection Attacks*

Cloud malware injection attack refers to a manipulated copy of the victim's service instance, uploaded by attacker to cloud, so that some service requests to the victim's service are processed within that malicious instance. An attacker can get access to user data

through this attack. The attacker actually exploits its privileged access capabilities in order to attack that service security domain. The incidents of this attack include credential information leakage, user private-data leakage and unauthorized access to cloud resources. The challenge does not only lie in the failure to detect the malware injection attack but also in the inability to determine the particular node on which the attacker has uploaded the malicious instance Retrospective detection (examination of hard-drive and memory) has been a widely used technique to detect the host of malware instances. According to the reference propose a new retrospective detection approach based on portable executable (PE) format file relationship. This approach has been implemented and validated in HADOOP platform. This approach proves higher detection rate as well as lower false positive rate. The main drawback of this approach is that its success is based on three assumptions (pre-requisites): (1) most legitimate programs and malware files are in PE format and lie within a windows platform; (2) the number of legitimate files is greater than that of malware files in user's computer; and (3) creating/writing/reading PE format files seldom happen in a user's computer. However, an attacker could exploit any vulnerability in cloud to attack without following any of these pre-requisites.

(1) most legitimate programs and malware files are in PE format and lie within a windows platform; (2) the number of legitimate files is greater than that of malware files in user's computer; and (3) creating/writing/reading PE format files seldom happen in a user's computer. However, an attacker could exploit any vulnerability in cloud to attack without following any of these pre-requisites. The authors fail to discuss the consequences of the absence of these pre-requisites such as (1) how efficient this approach would be if one or more of the assumptions are not fulfilled; (2) how much damage and attacker could cause to system or data in absence of these assumptions. CloudAV provides two main features that make it more efficient, accurate and fast as a malware detection system:

Antivirus as a network service: the detection capabilities by host-based antivirus can be more efficiently and effectively provided as cloud-network-service. Each host runs a light weight process to detect new files and then sends them to network service for quarantine and for further analysis rather than running complex analysis software on each end-host.

N-version protection: malicious software identification is determined by multiple heterogonous detection engines in parallel similar to the idea of N-version programming. The notion of Nversionprotection has been provided in this solution so that the malware detection system should leverage detection capabilities of multiple heterogeneous detection engines to determine malicious and unwanted files more effectively. However, the number of false positives encountered during normal operations increase compared to 1-version engines. To manage the false positives, the administrator has to set a trade-off between coverage (a single detector is enough to mark a file as malicious) and false positives (a consensus of a number of detectors is required to mark a file as malicious).

*E. Targeted Shared Memory Attacks*

In this attack, attackers take advantage of shared memory (cache or main memory) of both physical and virtual machines. It is an initial level attack in cloud computing that can lead up to several different types of attacks such as side channel attacks and malware injection attacks [53]. For example, authors in perform cross-virtual-machine-side-channels attack on Amazon EC2 and measure the cache activity of other users, which provides an example of activity-information leakage in cloud computing. Attackers can get unauthorized access to information that reveals the internal structure of the cloud such as the number of processes running, the number of users logged-in in a specific time and the temporary cookies residing in memory. Another example of targeted shared memory attack is explored by Rochsa and Correia in. The goal is to access the memory dumps in virtual machines through malicious insider attack. This access has led to the extraction of the current running processes in the system and users' private information.

Thus far, in the literature, no one has claimed to solve or prevent targeted shared memory attacks.Researchers and practitioners are working to get more information about the attack and no strong solution is available to prevent it except current anti-viruses or firewalls that limit users' access to the shared memory.

*F. Phishing Attacks*

Phishing is an attempt to access personal information from unsuspecting user through social Engineering techniques. It is commonly achieved by sending links of webpages in emails or through instant messages. These links appear to be correct, leading to a legitimate site such as bank account login or credit card information verification but they practically take users to fake locations. Through this deception, the attacker can obtain sensitive information such as passwords and credit card information. Phishing attacks can be classified into two categories an abusive behavior in which an attacker hosts a phishing attack site on cloud by using

one of the cloud services and hijack accounts and services in the cloud through traditional social engineering techniques Cloud security alliances (CSA) mentioned that cloud service providers do not maintain sufficient control over systems in order to avoid being hacked or spammed. To prevent such attacks, CSA proposes a few precaution measurements such as strict registration process, secure identity check procedure and enhanced monitoring skills. Privacy laws in cloud computing do not allow cloud service providers to look at what customers are doing, so if a malicious individual or organization is performing something nefarious (phishing attack or uploading malicious code) by using cloud services, it cannot be detected until or unless notified by some security software. Researchers discuss the fact that the present cloud privacy laws restrict cloud providers to become the first to know about nefarious activities
in their clouds, regardless of the enhanced monitoring and comprehensive inspection of network traffic.

## III. CONCLUSIONS

The adoption of cloud computing paradigm is continuously growing. In 2010, the IT spending in America to migrate to cloud computing solutions was estimated at $20 billion. Analysts believe that the cost reduction factor in cloud computing will further accelerate the adoption of cloud computing in the public sectors. With the massive growth in cloud computing adoption, the security attracted the attention of researchers and practitioners but still has not received enough attention. In this work, we conduct a survey on the current cloud security issues and the state-of-the-art security solutions. Then, we classify these issues into five security categories, namely: security standards, network, access, cloud infrastructure, and data. We also identify nine attack classes that target the clouds and present variable incidents of each attack such phishing, fate sharing, botnet, and malware injection. For each attack class, we present the state-of-the-art countermeasures and provide a comparative analysis of the effectivenessand the shortcomings of the proposed solutions. Finally, we present and evaluate the effectiveness ofthe state-of-the-art general countermeasures for cloud security attacks including intrusion detectionsystems, autonomous systems, and federated identity management systems. We also highlight the shortcomings of these systems that include the high communication and computation overhead and the detection efficiency and coverage.

## REFERENCES

[1] 1.Khalil, I. MCC: Mitigating colluding collision attacks in wireless sensor networks. In Proceedings of the 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA, 6–10 December 2010; pp. 1–5.
[2] M. Hayajneh, I. Khalil and Y. Gadallah, “An OFDMA-based MAC protocol for under water acoustic wireless sensor network,” Proceedings of the 2009 ACM International Conference on Wireless Communications and Mobile Computing (IWCMC’09), Leipzig, Germany, June 21 – 24 2009, pp. 810-814.
[3] Khalil, I.; Hayajneh, M.; Awad, M. SVNM: Secure verification of neighborhood membership in static multi-hop wireless networks. In Proceedings of the IEEE Symposium on Computers and Communications, 2009, ISCC 2009, Sousse, 5–8 July 2009; pp. 368–373.
[4] Sengupta, S.; Kaulgud, V.; Sharma, V.S. Cloud computing security—Trends and research directions. In Proceedings of the 2011 IEEE World Congress on Services (SERVICES), Washington, DC, USA, 4–9 July 2011; pp. 524–531.
[5] Samarati, P.; di Vimercati, S.D.C. Data protection in outsourcing scenarios: Issues and directions. In Proceedings of the 5th ACM Symposium on Information, Computer and CommunicationsSecurity (ASIACCS ’10), Chicago, IL, USA, 4–8 October 2010; ACM: New York, NY, USA, 2010; pp. 1–14.
[6] Popovic, O.; Jovanovic, Z.; Jovanovic, N.; Popovic, R. A comparison and security analysis of the cloud computing software platforms. In Proceedings of the 2011 10th International Conference onTelecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), Nis, Serbia,5–8 October 2011; Volume 2, pp. 632–634.
[7] Rachel Suresh, N.; Mathew, S.V. Security concerns for cloud computing in aircraft data networks. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions (ICITST), Abu Dhabi, United Arab Emirates, 11–14 December 2011; pp. 132–136.
[8] Fangfei, Z.; Goel, M.; Desnoyers, P.; Sundaram, R. Scheduler vulnerabilities and coordinated attacks in cloud computing. In Proceedings of the 2011 10th IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 25–27 August 2011; pp. 123–130.