International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

A Survey on SaaS-Attacks and Digital Forensic

Miss. Pallavi D. Katkule[1], Dr. B.B. Meshram[2]

[1] *Student, Dept. of Computer Engineering, Veermata Jijabai Technological Institute(VJTI), Maharashtra, India*
[2]*Professor, Dept. of Computer Engineering, Veermata Jijabai Technological Institute(VJTI), Maharashtra, India*

Abstract - *Software-as-a-service (SaaS) is one of the software service delivery model which encloses a broad range of business opportunities and challenges. Users and service providers are unwilling to consolidate their business into SaaS due to its security concerns while at the same time they are attracted by its benefits. Here different environments like cloud computing, mobile cloud computing, software defined networking and Internet of things related to SaaS utility and applicability are highlighted. It then commences on the analysis of SaaS security challenges spanning across data security, application security and SaaS deployment security, possible solutions or techniques which can be pertained in tandem are presented for a secure SaaS platform. This research is to identify the malicious activity in cloud base Software as Service (SaaS) environment. Besides investigating crimes related to the cloud environment in forensically sound manner, the process of conducting cybercrime investigation in the cloud environment is called as cloud forensics. This process is facing complex challenges because of the dynamic nature of cloud computing. Many algorithms and methodologies are there where security of data in cloud computing can be attained but at the same time it possesses many security risks. In this paper we identify different security attacks on cloud. More specifically this paper presents a detailed study of SaaS components' security and determines vulnerabilities and countermeasures. It also addresses a cloud forensic strategy is proposed for assisting digital investigators and experts for investigation of cybercrimes in effective and efficient manner.*

Key Words: *Cloud computing, SaaS attacks, Cloud Forensics, Cloud security challenges*

1. INTRODUCTION

Various cloud computing service providers are present with their services in the cloud environment. These services are available along with various specifications, features and methods of achieving security. Some services focus on secure access to a service and data by encryption, and some are focusing on secure network itself. Techniques acquired by various providers to achieve security are of varying nature. A cloud user may seek a service based on his requirement and level of security provided by a service. To analyze a particular service based on its various security properties is a challenge. The major challenge is to trust a cloud service or service provider in terms of security. One can attempt to model such „confidence" in a cloud service, as a kind of trust value. This thesis explores the possibility of building such a framework for trust computation, and its various aspects.

Solution to the definition of cloud computing is the "cloud" itself. For our purposes, the cloud is a large group of interconnected computers. These computers can be personal systems or network servers; they can be public or private. For example, Google hosts a cloud Google's cloud is a private one (that is, Google owns it) that is publicly accessible (by Google's users). Cloud computing means utilizing hardware and software resources that are delivered as a service over a network. Clouds authorize users to pay for whatever resources they use, allowing users to increase or decrease the amount of resources requested as needed. The framework design and characteristics of Cloud Computing imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability. While many traditional threats are encountered effectively, a number of security challenges and unchartered risks have been introduced to the clouds. There are many queries that appear as to whether a cloud is secure enough. Considering intruders there are many kinds of possible attacks, such as Denial of service attacks, Side Channel attacks, Authentication attacks, Man-in-the-Middle Cryptographic attacks, wrapping attacks, Malware-Injection attacks, flooding attacks, Browser attacks, and also Accountability checking problems. There is a critical need to securely store, manage, share and analyze massive amounts of complex (e.g., semi-structured and unstructured) data to determine patterns and trends in order to improve the quality of healthcare, better safeguard the nation and explore alternative energy and to provide solutions to detect top attack types using machine learning techniques. In this paper attempts are made to identify and analyze different types of attacks in cloud computing environment.

1.1 Overview of Cloud

Cloud Computing is a type of computing infrastructure that consists of a collection of interconnected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users.

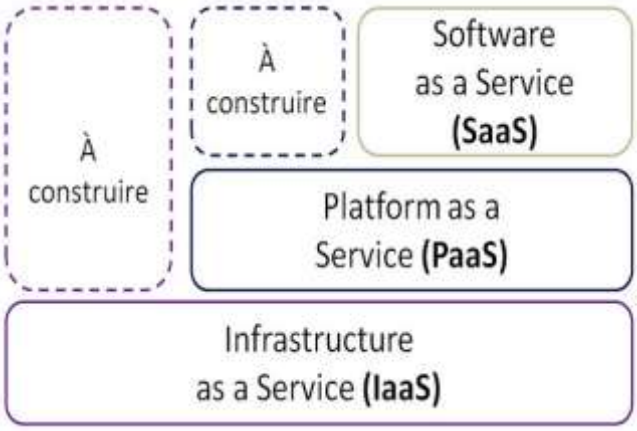

Fig-1: Cloud computing services

It focuses on delivering reliable, secure, fault-tolerant, sustainable, and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing virtually unlimited computing and storage, and hiding the complexity of large-scale distributed computing from users. Services are delivered over the Internet or private networks, or combination of these. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements. Depending on the type of service provided, there are three types of cloud services also termed as delivery models; Infrastructure as a service, (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

- IaaS deals with providing computing facility, storage or any other hardware resource. Amazon is one of the cloud providers offering IaaS. Examples of these services are EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service).

- PaaS provides platforms in terms of operating system and any other system software that can be used to build custom applications by the users. User can configure and develop their application on the specific platform. Microsoft Azure is an example of PaaS.

- SaaS deals with using any application or service via cloud. Google calendar is one of the examples that provide collaboration on various applications, like event management, project management etc. via internet. Salesforce is also a common and popular example of CRM SaaS Application.

A private cloud is one of the cloud computing deployment models that is dedicated to one organization to reduce costs and save time. This type of cloud is to provide computing services in a dynamic manner with direct control over the infrastructures. As shown in Figure 5.1,

"More enterprise workloads moved to both public and private cloud over the last year, with private cloud growing faster. The number of enterprises running more than 1,000 virtual machines (VMs) in public cloud increased from 13 percent to 17 percent, while those running more than 1,000 VMs in a private cloud grew from 22 percent to 31 percent. The private cloud growth in workloads also may include long-standing virtualized environments that have been enhanced and relabeled as a private cloud".

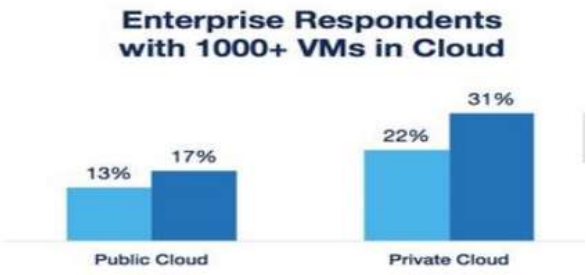

Fig-2: Enterprises respondents with 1000+VMS in Private and Public Cloud (Year 2017-18)

Need of performing Digital Investigation on the cloud platform leads propose a technique that will be able to prevent the unauthorized deletion of VM.

Common reasons include:

- Forensics in the Cloud scenario is a challenging task.
- To detect the retime attack generated by end user using IDS system.
- Preservation of evidences is the ultimate goal behind performing cloud forensics.
- In the Virtual Scenario, Virtual Machines contain evidences, it is impossible to recover your VM.
- In current scenario, if the VM is deleted intentionally or unknowingly it leads to the destruction of almost every evidence stored in it.

Thus, if becomes very important to prevent such an unauthorized deletion of VM by anyone which can aid both Security and Forensics in return.

1.2 Need

The proposed methods address security challenges in cloud computing and solutions to overcome these challenges. The following points can be observed from above related work:

1. Cloud computing is considered unsafe to be used by organizations and he also stated cloud computing requires some standards. This provides a need for further research to ensure security for all those who are using cloud computing applications.
2. System concluded in their article that security is always

addressed late while adopting cloud computing. It also says that no proper security standards for cloud computing exist.
3. Security challenges are still a major hindrance for adopting cloud computing
4. System identified some threats to cloud computing and proposed a method for automatic detection of network attacks, but it is still not used in real world.
5. Few security areas of cloud computing are identified to be less researched and also suggest to use another way of categorization in further studies.

2. ATTACKS ON CLOUD

The cloud is a booming technology in the computer sector. It refers to the accessing of the information technology and the software applications through the internet connection. The Software as a service (SAAS), Platform as a service (PAAS) and the Infrastructure as a service (IAAS) all together encapsulate to form the cloud. All the above services are the three types of services that is been provided by cloud computing. The services are hosted at the data centre by the cloud service providers for the organization or the individual users to utilize the services through a network connection. The cloud service providers are the companies that offer different services in the cloud.

The major cloud service providers include AWS, Sales force, Cisco, Apple, Google, IBM (Soft Layer), Oracle, Microsoft (Azure), and SAP, Rack space, and Verizon (which acquired Terre mark. But the Sales force and the Apple are interested in providing their own application rather than hosting applications for others. The companies like Google, IBM, Microsoft, SAP provides all the three services of the cloud while the other companies provide either two or one of the cloud services. One of the disadvantages in cloud computing is security attacks. This drawback is due to the data storage at different geographical areas in cloud computing**.**

The above chart describes the various security threats in public clouds as per the cloud security report provide by cloud security insiders, thus from the chart the misconfiguration of the cloud platform is about 62%, unauthorized access is about 55%, Insecure interfaces /APIs is about 50%, Hijacking of accounts, services or traffic is about 47%. In section 2, we discussed different types of attacks on the cloud such as denial of service, malware injection attack, side channel attack, authentication attack, a man in the middle attack. Section 3, describes various machine learning algorithm used in security attack to detect like naive Bayes, support vector machine (SVM), K-means clustering, fuzzy logic, decision tree, and genetic algorithm.

The cloud encounters many security attacks due to its disadvantages. The various cloud attacks like Denial of service attack, Malware injection attack, side channel attack, Man in the middle attack and the authentication attack are discussed below. The attacks may happen at different parts of the cloud like the data storage, during a transaction, during resource utilization and sharing. The loss of the attack can be lower to higher based on the type of attack. The reason for the attack in the cloud is due to the huge increase in the use of cloud services.

Denial of service attack

Denial of service attack the targeted cloud system is overloaded with the service requests from the attacker that stops it from responding to the upcoming new requests and to its users. According to some of the cloud security alliance, this cloud is very much vulnerable to this Dos attack. The Denial of service attack can be categorized into the DoS attack and the DDoS (Distributed denial of service attack). The attack was done using the single system and the single network is known as the DoS attack. The attack was done using multiple systems and the multiple networks are known as the Distributed denial of service attack (DDoS). The different types of the DDoS attacks are Volume based attack, protocol attacks, Application layer attack.

Malware injection attack

Malware injection attack the attacker injects the victim system with the malicious service or the malicious virtual machine. Here the attacker creates its own malicious virtual machine or the malicious service module and tries to add it into the cloud system. Then the attacker must behave so as to make the cloud system believe that it is a valid service. If the attacker succeeds, then the cloud automatically redirects all the requests to this malicious service. Now the attacker can access the service requests of the victim services.

Side channel attack

The attacker tries to compromise the cloud system by placing a malicious virtual machine nearby to the target cloud system then it dispatches the side channel attack. These channels are created in the software implementation of cryptographic algorithms. Its impact may be greater than any other attacks as they attempt to retrieve secret data without any special privileged access and in a non-exhaustive manner. There are different categories of side channel attack like Timing attacks, Cache attacks, Electromagnetic attacks, and Power-monitoring attacks. Electromagnetic attacks and power – monitoring attacks are mostly applicable to physical devices such as smart cards. The cache attacks and the Timing attacks are mainly applicable to the cloud computing.

Authentication attack

The Authentication attack mainly focuses on the authentication part of the cloud services. The primary authentication in most of the services is the username and the password which is a type of the knowledge-based authentication. The secondary authentication like shared secret questions, site keys, virtual keyboards is used by secure functioning organizations like the financial company. Some of the authentication attacks are the Brute Force Attacks, Dictionary Attack, Shoulder Surfing, Replay Attacks, Phishing Attacks, Key Loggers.

a) Brute force attack: This attack is like a trial and error method; all possible combinations of the password are applied to break the password.

b) Keyloggers: It is a form of a software program, where it monitors the actions of the user by recording each and every key pressed by the user.

c) Phishing attack: In this attack, the attacker redirects the user to the fake websites to get the passwords and the pin codes of the user, it is a kind of the web-based attack.

Man-in-the-middle-attack

Man-in-the-middle attack the attacker intercepts the message in the public key exchange and retransmits it by substituting its own public key for the requested one, but the two original are still communicating normally. The sender does not know that the messages sent by him is received by an attacker and he can access data, modify the message before retransmitting it to the receiver. Some of the man-in-the-middle attacks are Address Resolution Protocol Communication (ARP), ARP Cache Poisoning, DNS Spoofing, Session Hijacking.

3. PROPOSED FORENSIC MODEL

The idea of the proposed model is that the CSP stores logs of a VM whose activities are identified as malicious by an intrusion detection system. Simultaneously the CSP should be requested for log files of the suspected VM and the investigator collects and processes the log files to obtain the evidence.

To collect proper and correct evidence, the suspected VM should be monitored for some more time after it is identified to be performing malicious activities. The more time the suspected VM is monitored the more it can be sure of the possibility of malicious behavior. Once the investigator identifies the sources of evidence, the suspicious VM is moved to other nodes to preserve confidentiality, integrity and authenticity of other VMs. By moving or isolating, VM evidence can be protected from contamination and tampering. Below Figure shows the proposed approach to perform forensic investigation using VM logs as evidence.

The proposed research work has been distributed into 3 different stages these are below:

Modules Used

A. Intrusion Detection Systems:

Intrusion detection systems (IDS) are used to alert users of an attack. These systems monitor a specific system in order to gather and analyses information to determine whether there is a security threat. These security threats can range from something as begin as someone mistyping a password to something malevolent as a Denial of Service attack.

In order to maximize the efficiency of checking for security threats, IDSs are specialized to handle specific components. For instance, there are network IDSs which specialize in monitoring network traffic for malicious activity.

B. Snapshots:

A "snapshot" is capable of capturing a machine in its current state. They are typically used so that a user can easily back up current configurations of their IaaS machine before attempting to install software or reconfiguring software that may break the machine. This session log capability is offered by many hypervisors and CSPs.

C. Log based Approach:

In digital world, log is a regular or systematic record of actions that object has taken. It is the most common component that can be used in digital forensics.

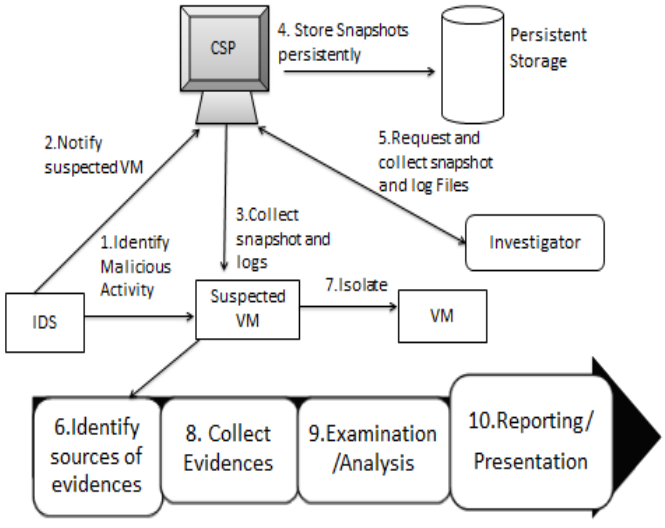

Fig-3: Proposed System

4. IMPLEMENTATION DETAILS

1. Java

Java is –

- Object Oriented – In Java, everything is an Object. Java can be easily extended since it is based on the Object model.
- Platform Independent – Unlike many other programming languages including C and C++, when Java is compiled, it is not compiled into platform specific machine, rather into platform independent byte code. This byte code is distributed over the web and interpreted by the Virtual Machine (JVM) on whichever platform it is being run on.
- Simple – Java is designed to be easy to learn. If you understand the basic concept of OOP Java, it would be easy to master.
- Secure – With Java's secure feature it enables to develop virus-free, tamper-free systems. Authentication techniques are based on public-key encryption.

2. Eclipse

There are many ways to learn how to program in Java. The most developers believe that there are advantages to learning Java using the Eclipse integrated development environment (IDE). Some of these are listed below:

- Eclipse provides a number of aids that make writing Java code much quicker and easier than using a text editor. This means that you can spend more time learning Java, and less time typing and looking up documentation.
- The Eclipse debugger and scrapbook allow you to look inside the execution of the Java code. This allows you to "see" objects and to understand how Java is working behind the scenes
- Eclipse provides full support for agile software development practices such as test-driven development and refactoring. This allows you to learn these practices as you learn Java.

3. Java Development Kit (JDK)

- The Java Development Kit (JDK) is an implementation of either one of the Java SE, Java EE or Java ME platforms released by Oracle Corporation in the for of a binary product aimed at Java developers on Solaries, Linux, Mac OS X orWindows.
- Since the introduction of Java platform, it has been by far the most widely used Software Development Kit (SDK) on 17 November 2006; Sun announced that it would be released under the GNU General Public License (GPL), thus making it free software. This happened in large part on 8 May 2007, when Sun contributed the source code to open JDK.

4. MySQL

- MYSQL is the open source SQL database, which is developed by Swedish company MySQL. MySQL is pronounced as" my ess-que-ell," in contrast with SQL, pro- nounced" sequel." MySQL is supporting many different platforms including Microsoft Windows, the major Linux distributions, UNIX, and Mac OS MySQL has free and paid versions, the major Linux distributions, UNIX, and Mac OS MySQL has free and paid versions, depending on its usage (non-commercial/commercial) and features. MySQL comes with a very fast, multi-threaded, multi-user, and robust SQL database server.

Following are the features of MySQL:

- High Performance
- High Availability
- Scalability and Flexibility Runs anything
- Robust Transactional Support
- Strong Data Protection

5. RESULT

Fig-4: Using Eclipse as a Cloud support for web app

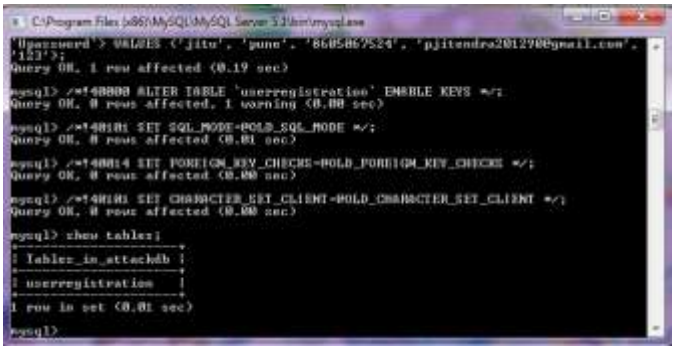

Fig-5: Working of MySQL

Fig-6: User login to the website

Fig-7: Session Hacking Attack

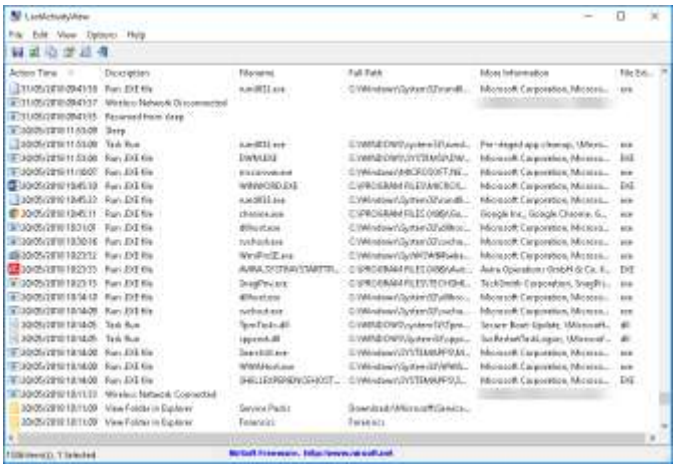

Fig-8: Reading Log Files

6. CONCLUSION

Addressing the security, privacy and trust challenges of cloud computing is a complex undertaking since it requires a combination of technological solutions and legal approaches that is capable of addressing operational realities and concerns. In this paper we investigated these challenges and proposed many recommendations such as Establish International organization for Cloud Crimes, vetting cloud service providers, Personal encryption method, Permissions for data tracking, Localization, Personal security service to increase security and trust also maintaining privacy. But it should be noted that, security and privacy can never be assured and secured 100% in these areas.

Future Work

In the domain of Cloud there always remains a room for enhancement in the existing system. At present the work was successful in integrating the proposed system with the command line interface. Thus, in future, efforts for integration of an authentication mechanism with the graphical user interface of cloud would be undertaken.

REFERENCES

[1] N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, New Delhi, 2016, pp. 243-250.

[2] E. Morioka and M. S. Sharbaf, "Digital forensics research on cloud computing: An investigation of cloud forensics solutions," *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2016, pp. 1-6.

[3] M. U. Bokhari, Q. M. Shallal and Y. K. Tamandani, "Security and privacy issues in cloud computing," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 896-900.

[4] A. Albugmi, M. O. Alassafi, R. Walters and G. Wills, "Data security in cloud computing," *2016 Fifth International Conference on Future Generation Communication Technologies (FGCT)*, Luton, 2016, pp. 55-59.

[5] G. Kulkarni, N. Chavan, R. Chandorkar, R. Waghmare and R. Palwe, "Cloud security challenges," *2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, Bali, 2012, pp. 88-91.

[6] Karnwal, Tarun, T. Sivakumar, and G. Aghila. "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack." 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science. IEEE, 2012.

[7] Subashini, Subashini, and VeerarunaKavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.
[8] Tsai, Hsin-Yi, et al. "Threat as a service? Virtualization's impact on cloud security." IT professional 14.1 (2012): 32-37
[9] Zunnurhain, Kazi, and S. Vrbsky. "Security attacks and solutions in clouds." Proceedings of the 1st international conference on cloud computing. 2010.
[10] Cusumano, Michael A. "Cloud computing and SaaS as new computing platforms." Commun. ACM 53.4 (2010): 27-29.
[11] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Yousef, The Eucalyptus Open-Source Cloud Computing System. 2009 9th IEEEACM International Symposium on Cluster Computing and the Grid, 2009, p.124–131.
[12] Z.A. Khalifehlou, F.S. Gharehchopogh, Security Directions in cloud Computing Environments, 5th International Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara, Turkey, 17-19 May 2012, p.327-330.
[13] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.
[14] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3 No. 4, 2011, p. 2672-2676.
[15] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Procedia Engineering, Vol. 23, p.586-593, Elsevier, 2011.
[16] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, Volume 28, Issue 3, March 2012, P. 583–592.
[17] M. Monsef, N. Gidado, Trust and privacy concern in the Cloud, 2011 European Cup, IT Security for the Next Generation, 2011, p.1-15.