International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

SAAS Attacks Defense Mechanisms and Digital Forensic

Prasad Garad[1], Dr. B. B. Meshram[2]

[1]PG Student Department of Computer Engineering, Veermata Jijabai Technological Institute, Mumbai.
[2]Prof. Department of Computer Engineering, Veermata Jijabai Technological Institute, Mumbai.

Abstract - *Software-as-a-service (SaaS) is a type of software service delivery model which encompasses a extensive range of business opportunities and challenges. Users and service providers are unenthusiastic to integrate their business into SaaS due to its security concerns while at the same time they are attracted by its benefits. This article highlights SaaS utility and applicability in different environments like cloud computing, mobile cloud computing, software defined networking and Internet of things. It then embarks on the analysis of SaaS security challenges spanning across data security, application security and SaaS deployment security, possible solutions or techniques which can be applied in tandem are presented for a secure SaaS platform. This research 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 performing cybercrime investigation in the cloud environment is known as cloud forensics. This process is facing complex challenges due to the dynamic nature of cloud computing. It also address a cloud forensic strategy is proposed for assisting digital investigators and experts for investigation of cybercrimes in effective and efficient manner. The proposed strategy is based on cloud computing platform that providing enormous processing and storage capabilities. This strategy can be as guided to the digital investigators and practitioners to follow it in performing of investigation of SaaS attacks*

Key Words: *SAAS, Network Attacks, DDOS attack, Forensic approach.*

1. INTRODUCTION

Cloud computing has become a part of the competitive market today. Many organizations utilize cloud administrations. Despite the fact that distributed computing administrations is developing and picking up notoriety, the dread about the utilization of cloud administrations is as yet an open issue. Different issues hindering appropriation are distinguished in the writing; one of the real ones is security. Security hazards in the territory of distributed computing has stood out since its start. New conventions and apparatuses are consistently sought after to improve the security quality of a distributed computing administration or specialist organization

Different distributed computing specialist co-ops are accessible with their administrations in the cloud condition. These administrations join different determinations, highlights and techniques for accomplishing security. A few administrations center around secure access to an administration and information by encryption, and some are concentrating on secure system itself. Procedures received by different suppliers to accomplish security are of shifting nature. A cloud client may look for an administration dependent on his necessity and level of security given by an administration. To dissect a specific administration dependent on its different security properties is a test. The real test is to believe a cloud administration or specialist organization as far as security. One can endeavor to show such „confidence" in a cloud administration, as a sort of trust esteem. This theory investigates the likelihood of structure such a framework for trust computation, and its various aspects.

1.1 Related work

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. 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).

2. LITERATURE SURVEY

Providing Security and Integrity for Data Stored In Cloud Storage [1] cloud computing is the computing paradigm which enable obtaining resources like software, hardware, benefits over the web. A large portion of client store their information on cloud for information security and uprightness are prime related. In this article the issue of guaranteeing information uprightness and security of information stockpiling in distributed computing. For guaranteeing accuracy of information, we expect the assignment of permitting a Third gathering examiner (TPA) utilized for uncovering danger of distributed storage benefits in the interest of the cloud customer to check information honesty put away in the cloud. This paper center around the information security, we proposed deletion revising code in

the document conveyance to give the redundancies and assurance information trustworthiness. By utilizing homomorphic token with disseminated check of eradication coded information, our plan accomplish capacity rightness just as mistake restriction. Broad security examination demonstrate the proposed plan is profoundly proficient and strong against Byzantine disappointment, vindictive information variation assault and considerably server intriguing assaults.

Asigra [2] presents another plan for reinforcement arrangement called agentless reinforcement and recuperation. Not at all like operator reinforcement arrangement which requires a reinforcement specialist introduced on the machine that necessities to reinforcement, agentless reinforcement as a rule introduces customer programming on one server which can remotely sign into an objective reinforcement framework and transmit the information to the focal stockpiling area. The benefit of agentless reinforcement is accommodation. Along these lines, specialist co-ops don't need to oversee operators introduced on every customer machines. The hindrances of this methodology are that agentless reinforcement is as yet not experienced enough and the server with agentless customer programming may open another assault vector for the programmers.

NIST Cloud Computing Forensic Science Challenges [3] distributed computing is a model for empowering universal, helpful, on-request system access to a common pool of configurable processing assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with negligible administration exertion or specialist organization connection. A total depiction and meaning of Cloud Computing is given in NIST SP 800-145 (connect is outside). Distributed computing can possibly offer cost investment funds both as far as capital costs and operational costs, just as influence driving edge innovations to meet the data handling needs of clients in people in general and private segments. Be that as it may, the adjustment in specialized activities and control elements (both as far as proprietorship and the board) as for IT assets presents new scientific science challenges.

Situation based Design for a Cloud Forensics Portal [4] the point of computerized crime scene investigation is to extricate data to answer the 5Ws (Why, When, Where, What, and Who) from the information separated from the proof. So as to accomplish this, most computerized criminological procedures expect total control of advanced proof. Notwithstanding, in a cloud domain legal examination, this isn't constantly conceivable. Furthermore, the novel qualities of distributed computing make new specialized, lawful and building difficulties when leading a legal examination. We propose a theoretical situation to reveal and clarify the difficulties criminological professionals face during cloud examinations. Furthermore, we additionally give answers for location the difficulties. Our theoretical case situation has demonstrated that, over the long haul, better live scientific apparatuses, improvement of new techniques custom fitted for cloud examinations and new strategies and models are in reality required. Moreover, we have reached the resolution that criminological examinations greatest test isn't specialized however legitimate.

The creators in [5] proposed a high-accessibility and uprightness layer (HAIL) for cloud information stockpiling. It is a remote information uprightness checking convention to guarantee information respectability and accessibility through an interleaving of various kinds of mistake remedying layers which influence dispersal code, server code and total code. The restriction of this methodology is that it can just give confirmation to static information.

As per SaaS applications [6] are generally utilized and overseen over the web. They are introduced to clients in a program. This makes it unavoidable to go up against the security difficulties, for example, SQL infusion, Cross-site scripting and Cross-site Request Forgery. Programming interface is the foundation of SaaS stage which plans to manage heterogeneity and permit robotization of regular procedure that cooperate with administrations running on another machine. The advantage of API to SaaS is critical, however it is likewise tormented with security issues. Inadequately coded APIs can be effectively manhandled or abused by an assailant. Web administration is a product framework intended to help machine-to-machine communication over system. WSDl and SOAP are utilized to a great extent by SaaS applications, normally passed on utilizing HTTP with a XML serialization. These procedures, notwithstanding, are observed to be defenseless against different assaults. for example, XML wrapping assaults and WSDL checking.

Cloud Forensics: Evidence Collection and Preliminary Analysis [7] Cloud registering frameworks have a large portion of the present business applications yielding it high income which makes it an objective of digital assaults. This underlines the requirement for an advanced legal instrument for the cloud condition. Regular computerized crime scene investigation can't be legitimately exhibited as a cloud measurable arrangement due to the multi tenure and virtualization of assets pervasive in cloud. While we do cloud crime scene investigation, the information to be assessed are cloud part logs, virtual machine plate pictures, unstable memory dumps, support logs and system catches. In this paper, we have thought of a remote proof gathering and pre-preparing structure utilizing Struts and Hadoop conveyed document framework. Gathering of VM plate pictures, logs and so forth., are started through a force model when activated by the specialist, while cloud hub intermittently pushes system catches to HDFS. Pre-handling steps, for example, grouping and relationship of logs and VM circle pictures are brought out through Mahout and Weka to actualize cross drive examination.

A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing [8] Performing computerized criminology in cloud can add another measurement to the way toward structure trust in cloud. Be that as it may, the very qualities of cloud, for example, absence of straightforwardness, virtualization, lawful issues and so forth., present difficulties to cloud legal sciences. Regardless of whether it is conventional advanced legal sciences or cloud crime scene investigation, gathering thorough information for examination is a noteworthy test in examination. Information gathering in profoundly virtualized situations like cloud is exceptionally mind boggling. A definitive objective of proof gathering and investigation is to demonstrate to the official courtroom that they are forensically solid. We can utilize thoughtfulness strategies since these won't sully the condition of the wellspring of proof while gathering the required information. We recognized two noteworthy disadvantages in the reflection procedure. Initial, a legitimate activating condition will just make the agent to get the required information. Neglecting to devise legitimate triggers will prompt loss of information in the cloud multi-occupant condition. Next, during the information accumulation the comparing virtual machine (VM) must be delayed for some time, prompting execution debasement. In this paper, we stress for the most part on the primary issue and propose a structure for the contemplation of virtual machines to address the equivalent.

Advanced Evidence Detection in Virtual Environment for Cloud Computing [9] Cloud registering frameworks give a worldview to the conveyed handling of computerized information. Computerized legal examinations including such frameworks are probably going to include progressively complex advanced proof procurement and investigation. Some open distributed computing frameworks may include the capacity and handling of computerized information in various purviews, and a few associations may scramble their information before it enters the cloud. Both of these variables related to cloud designs may make scientific examination of such frameworks increasingly mind boggling and tedious. There are no settled advanced measurable rules that explicitly address the examination of distributed computing frameworks. In this paper we look at the legitimate parts of advanced measurable examinations of distributed computing frameworks.

Helped Deletion of Related Content [10] on essential stockpiling frameworks substance is frequently imitated, changed over or altered, and the clients rapidly lose power over its dispersal on the framework. Erasing substance identified with a specific venture from the framework in this way turns into a work serious errand for the client. In this paper we present IRCUS, a framework that helps the client in safely evacuating undertaking related substance, yet does not expect changes to the client's conduct or to any of the framework segments, for example, the record framework, piece or applications. IRCUS straightforwardly coordinates inside the client's framework, works in client space and stores the subsequent metadata alongside the files. We implemented and evaluated our system and show that its overhead and accuracy are acceptable for practical use and deployment.

3. PROPOSED SYSTEM

We propose a protected information sharing arrangement for component people. At first, we propose an ensured way for key scattering with safe correspondence channels, and the customers can securely get their private keys from social occasion boss. In our proposed framework we utilize three distinct elements information proprietor, bunch director, cloud server and aggressor is untrusted substance. In this module first information proprietor transfer the information document to cloud server utilizing cryptography calculation once information has store into database, proprietor gets the notice about record stockpiling effectively. The information proprietor having a full access of explicit information document he can share or access, so information proprietor can share the any record to any gathering supervisor then it will consequently access to all gathering individuals. The common gathering individuals can get to each record to whenever by cloud server. In first stage on the off chance that information proprietor deny any client from access the document, at that point he can't access such record. On the off chance that he can attempt to produce any conspiracy assault utilizing SQL infusion inquiries, even our framework will framework will counteract such assaults. Second information proprietor can share and deny document to singular client to explicit gathering, and third once any user revoke system will automatically generate proxy key generation that means existing keys will expired. The overall approach improves the system efficiency as well security on drastic level.

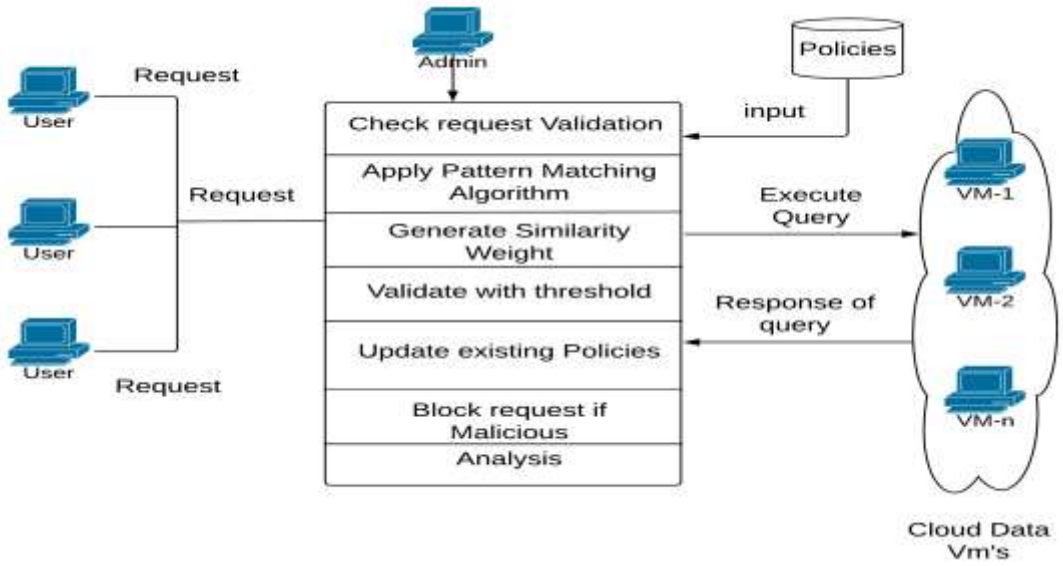

Figure 1. Proposed system architecture

The above figure a shows the system architecture of proposed system where we carried below attack detection as well as prevention of system.

1. SQL Injection

Injection attacks happen when untrusted data is sent to a code interpreter through a structure info or some other information accommodation to a web application. For instance, an aggressor could enter SQL database code into a structure that expects a plaintext username. In the event that that structure information isn't appropriately verified, this would bring about that SQL code being executed. This is known as an SQL injection attack.

2. Cross-Site Scripting

Cross-site scripting vulnerabilities occur when web applications allow clients to include custom code into a url way or onto a site that will be seen by different clients. This helplessness can be abused to run vindictive JavaScript code on an unfortunate casualty's program. For instance, an assailant could send an email to an injured individual that gives off an impression of being from a confided in bank, with a connection to that bank's site. This connection could have some malevolent JavaScript code labeled onto the finish of the url. In the event that the bank's website isn't appropriately ensured against cross-webpage scripting, at that point that vindictive code will be kept running in the unfortunate casualty's internet browser when they click on the connection.

Alleviation procedures for cross-site scripting incorporate getting away untrusted HTTP demands just as approving as well as sterilizing client produced content. Utilizing current web advancement systems like ReactJS and Ruby on Rails likewise gives some inherent cross-website scripting security.

JavaScript cross-site scripting assaults are mainstream in light of the fact that JavaScript approaches some touchy information that can be utilized for wholesale fraud and different vindictive purposes. For instance, JavaScript approaches cookies*, and an assailant could utilize a XSS assault to take a client's treats and mimic them on the web. JavaScript can likewise make HTTP demands, which can be utilized to send information, (for example, stolen treats) back to the aggressor. Moreover, customer side JavaScript can likewise enable an assailant to get entrance to APIs that contain geo location coordinates, webcam data, and other sensitive information.

3. Insufficient Logging And Monitoring

Many web applications are not taking enough steps to detect data breaches. The average discovery time for a breach is around 200 days after it has happened. This gives attackers a lot of time to cause damage before there is any response. OWASP suggests that web designers should execute logging and checking just as occurrence reaction intends to guarantee that they are made mindful of assaults on their applications. Lacking logging and checking weakness happens when the security-basic occasions aren't logged appropriately, and the framework isn't observing the present happenings. Unquestionably, the absence of these functionalities can make the malevolent exercises harder to identify and it influences successful episode taking care of when an attack happens.

Companies are maintaining the log files to deliver a continuous trace of everything, which happens with their systems and data. Collecting log data are generally recommended as a security industry best practice. In addition to that, several regulations mandate the assembly, storage, and evaluation of logs.

Prevention terminologies

- Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.
- Establish or adopt an incident response and recovery plan

Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.

4. Sensitive Data Exposure

If web applications don't protect sensitive information, for example, money related data and passwords, aggressors can access that information and sellor use it for detestable purposes. One prominent strategy for taking delicate data is utilizing a man-in-the-center assault.

Information presentation hazard can be limited by encoding every single touchy datum just as handicapping the storing of any delicate data. Moreover, web application designers should take care to guarantee that they are not superfluously putting away any delicate information.

Reserving is the act of briefly putting away information for re-use. For instance, internet browsers will frequently reserve site pages so that if a client returns to those pages inside a fixed time range, the program does not need to get the pages from the web.

The principal thing is to decide the security needs of information in travel and very still. For instance, passwords, Visa numbers, wellbeing records, individual data and business insider facts require additional insurance, especially if that information falls under protection laws, for example EU's General Data Protection Regulation (GDPR), or guidelines, e.g. financial data protection such as PCI Data Security Standard (PCI DSS). For all such data:

- Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, and FTP. External internet traffic is especially dangerous. Verify all internal traffic e.g. between load balancers, web servers, or back-end systems.
- Are any old or weak cryptographic algorithms used either by default or in older code?
- Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing?
- Is encryption not enforced, e.g. are any user agent (browser) security directives or headers missing?
- Does the user agent (e.g. app, mail client) not verify if the received server certificate is valid?

5. Security Misconfiguration

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could demonstrate a client excessively expressive mistakes which may uncover vulnerabilities in the application. This can be relieved by expelling any unused highlights in the code and guaranteeing that mistake messages are increasingly broad. Current application security designs don't pursue security as a matter of course. Actually, software engineers must apply safety efforts to keep away from access to private or secret assets.

On the off chance that Directory posting isn't debilitated on the server and in the event that assailant finds the equivalent, at that point the aggressor can just rundown indexes to discover any document and execute it. It is additionally conceivable to get the genuine code base which contains all your custom code and after that to locate a genuine imperfections in the application. Application server arrangement permits stack follows to be come back to clients, conceivably uncovering basic imperfections. Aggressors snatch those additional data that the blunder messages give which is sufficient to them to enter. Application servers as a rule accompany test applications that are not all around verified. If not expelled from creation server would bring about bargaining your server. Security Misconfiguration is essentially characterized as neglecting to actualize all the security controls for a server or web application, or executing the security controls, yet doing as such with blunders. What an organization thought of as a protected situation really has hazardous holes or errors that leave the association open to chance. According to the OWASP top 10, this type of misconfiguration is number 6 on the list of critical web application security risks.

6. URL Injection

URL injection is when a malicious individual attacks your website through the inclusion of risky code that takes

approval of client to enter in the site. It is otherwise called URL Manipulation Attacks. URL infusion, or vindictive connection inclusion. Directions in WordPress are sent through URL parameters, which programmers can undoubtedly twist and mishandle — causing WordPress to act without approval, or confound its activity. In straightforward terms, URL infusions occur when an individual endeavors to control your online database through the directions sent by the URL. Regularly, this type of hacking includes the production of new pages all through your site by programmers — frequently containing perilous bits of code or spam connects that can make your site a security hazard to guests. Regularly, the new pages that are made are pressed brimming with code that re-guides your guests to risky areas, or permits your webserver to partake in assaults that you may not know about.

There are various manners by which an aggressor can access your site — from misusing powerless or more seasoned adaptations of programming, to using unreliable indexes, or hacking various outsider modules – something especially normal **in WordPress. What that hacker does with your website when they gain access can leave you in serious trouble.**

4. CONCLUSION

In this work, we have proposed a novel approach Software as a Service (SaaS) i.e. Online Book Store is deployed on the web application server. It explains SaaS specific security challenges and how contemporary security testing can ensure that the challenges are met. Various vulnerabilities on SaaS application have been found which may results into attacks like Sensitive data exposure, security misconfiguration, XSS, Insufficient Logging and Monitoring, SQLi and URL Injection attacks. Security of any cloud-based services must be closely reviewed to understand what protections our information has. To enable digital in the cloud environment with respect to performance by taking VM session also we have provided the prevention mechanism for each attack. The cloud will be implemented for SaaS i.e. Book store, hence improves the performance of cloud.

REFERENCES

[1] Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari "Providing Security and Integrity for Data Stored In Cloud Storage" ICICES, 2014.

[2] "Agentless backup is not a myth," 2011.

[3] NIST, "NIST Cloud Computing Forensic Science Challenges", National Institute of Standards and Technology Interagency or Internal Report 8006, 2014.

[4] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky "Scenario-based Design for a Cloud Forensics Portal" IEEE, 2015.

[5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.

[6] M. Jensen, N. Gruschka, and R. Herkenhoner,¨ "A survey of attacks on web services," Computer Science-Research and Development, vol. 24, no. 4, pp. 185–197, 2016.

[7] Saibharath S, Geethakumari G "Cloud Forensics: Evidence Collection and Preliminary Analysis" IEEE, 2015

[8] BKSP Kumar RajuAlluri, Geethakumari G"A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing" IEEE, 2015.

[9] Mr. DigambarPowar, Dr. G. Geethakumari "Digital Evidence Detection in Virtual Environment for Cloud Computing" ACM, 2012.

[10] Hubert Ritzdorf, NikolaosKarapanos, SrdjanCapkun "Assisted Deletion of Related Content"ACM, 2014.