International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Challenges and Solutions to Impart Security on Software as A Service Model of Cloud Computing

Kranthi Kumar Rudrarapu, L. Jai Vinita, Dr. P. Neelakantan
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India

ABSTRACT

The buzzword in the IT business enterprise in recent times is cloud computing and it has a potential impact on several business applications as well as in our regular life. Many of the abilities that make cloud computing attractive have now not certainly challenged the existing security system, however, have additionally determined out new security issues. This paper gives an insightful evaluation of the existing fame on cloud computing protection issues based totally on a detailed survey and it additionally makes an try and describe the protection dreadful conditions in software as a service (SaaS) version of cloud computing and additionally endeavours to offer destiny safety research instructions.

Keywords: Cloud Computing, software as a service, security

I. INTRODUCTION

A lot has been written and spoken approximately Cloud Computing technology, by using IT specialists, enterprise and business leaders and impartial professionals. whilst a few believe it's far a disruptive fashion representing the next degree in the evolution of the net, others believe it's far hype, because it makes use of in advance installed computing technologies. So, what exactly is cloud computing? From a consumer attitude, cloud computing gives a means for obtaining computing services without any need for deep knowledge of the underlying era being used. From an organizational attitude, cloud computing can provide services for customer and commercial enterprise wishes in a simplified manner, providing unbounded scale and differentiated exceptional of service to foster speedy innovation and choice making.

According to Gartner [7], cloud computing may be described as ‘‘a fashion of computing, in which massively scalable IT- enabled capabilities are introduced ‘as a carrier’ to external clients using internet technologies. according to [8] and National Institute of standards and technology [3], guidelines for cloud computing, it has four one-of-a-kind deployment models specifically non-public, network, public and hybrid in addition to 3 exclusive delivery fashions which can be utilized within a specific deployment version. those transport fashions are the SaaS (software as a service), PaaS (Platform as a service) and IaaS (Infrastructure as a service). these models form the middle of the cloud and they show off sure key characteristics like on demand self-service, wide community access, resource pooling, measured service and rapid elasticity. Our predominant area of issue on this paper is the software as a service (SaaS). version .

This high-quality-regarded department of cloud computing , is a shipping model wherein applications are hosted and controlled in a service company's datacentre, paid for on a subscription foundation and accessed through a browser over a web connection. It basically deals with licensing of an utility to the customers for use as a service on call for. One right instance of SaaS is the Salesforce.com CRM utility.

SaaS (software as a service), PaaS (Platform as a service) and IaaS (Infrastructure as a service). these services are the fundamental models of the cloud. They occur crucial traits which include on-call for self-carrier, extensive community access, resource pooling, fast Elasticity and Measured carrier. in this paper, we are focusing on software as a service(SaaS) model. In trendy digital global, software -as-a-service (SaaS) normally refers to a brand new and alternative manner

of getting access to software, instead of more traditional methods of getting right of entry to while inside the beyond software program would commonly be purchased outright and loaded onto a tool, SaaS commonly refers to a subscription-based totally model in which the software is hosted inside the cloud and accessed through the browser with the internet connection. there are various benefits to consumers, who are individuals the use of the software program for personal functions, or agencies for public functions. there are many famous examples of SaaS, which includes office 365, Google Apps, Salesforce, Citrix GoToMeeting, Cisco WebEx and Netflix.

In this paper, there was s a focus on the security demanding situations associated with SaaS delivery model. The agency of the paper is as follows: phase 2 describes the safety issues which might be posed by the software as a service (SaaS) delivery model. segment 3 lists some of the contemporary answers which partly goal the security challenges posed via the SaaS. phase four affords conclusions derived out of the survey undertaken.

II. SECURITY ISSUES RELATED TO SAAS

In a conventional on premise software deployment model, the private information of each employer persists to reside inside the organizational boundary and which problem to its personnel protection and access control regulations, logical and physical. nonetheless, inside the software program as a service version, the organization statistics are saved past the organizational boundary. in the end, the SaaS provider must tackle extra security regulations to prevent statistics protection and vulnerabilities because of safety exposures in the software. records place, facts Disposal, information Integrity, facts Confidentiality, authorization and authentication, network assaults and records availability are the demanding situations of SaaS service model.

Traditional security challenges:

The use of cloud computing introduced new attack vectors to be able to make assaults both feasible or simple to perform, despite the safety worries within the traditional communique structures which incorporates cloud. A number of the traditional safety issues which additionally, have an effect on the SaaS version which has been described underneath:

Authorization and authentication

The authentication and authorization applications for corporation environments may additionally need to be modified, to form a safe cloud environment. Forensics obligations may additionally grow to be a great deal extra tough for the reason that investigators may not be able to get physical access to the hardware of the system. The layout proposed by [5] lets in person to use a single set of credentials. they have got proposed an answer with de-facto requirements of open authorization in which there is a trust party auditor which continues all the credentials and cloud company can uniquely distinguish one person from other. The version proposed within the literature [6] verifies consumer authenticity the usage of -step verification, that is primarily based on password, smartcard and out of band (i.e. strong two elements) authentication. in addition, the scheme also offers mutual authentication, identification control, session key established order, personal privacy and security.

Availability

The supply ensures the dependable and timely access to cloud records or cloud computing assets via the right employees. the availability of cloud carrier providers is likewise a huge subject, considering if the cloud service is disrupted; it affects greater clients than within the conventional version. For instance, the recent disruption of the Amazon cloud carrier in the 12 months 2011, took down more than a few of websites such as Reddit, Foursquare, and Quora.The SaaS software providers are required to make sure that the structures are running nicely whilst wanted and organizations are supplied with offerings around the clock. This involves making architectural changes at the software and infrastructural levels to add scalability and high availability.

Resiliency to hardware/software program screw-ups, in addition to denial of service attacks, wishes to be built from the floor up within the software. at the same time, the precise movement plan for business continuity and catastrophe restoration (CR) wishes to be considered for any exigencies as in keeping with the guidance supplied by [8]. This is vital to make certain the protection of the company facts even as maintaining minimal downtime for the establishments. With Amazon as an example, the Amazon net offerings (AWS) API endpoints are hosted on the same net-scale, global-magnificence infrastructure that supports the

Amazon retail website. standard dispensed Denial of provider (DDoS) mitigation strategies which include synchronous cookies and connection restricting are used. To similarly mitigate the impact to capability DDoS assaults, Amazon maintains internal bandwidth that exceeds its issuer-furnished net bandwidth.

Data confidentiality

Confidentiality refers to the prevention of intentional or accidental unauthorized disclosure of facts. Confidentiality in cloud machine is associated with the regions of highbrow property rights, covert channels, traffic evaluation, encryption, and inference [12]. Cloud computing involves the sharing or storage of data on far-off servers owned or operated by means of others, whilst accessing the internet or any other connections. Cloud computing offerings exist in lots of variations, inclusive of records storage websites, video websites, tax instruction sites, private health report websites and much greater. The whole contents of a person's storage tool may be saved with a single cloud provider or with multiple cloud vendors. whenever a person, an enterprise, a central authority organization, or some other entity shares statistics inside the cloud, privacy or confidentiality questions rise up.

Virtual machine safety

Although the global adoption of virtualization is a particularly a current phenomenon, threats to the virtualized infrastructure are evolving simply as fast [7]. The hypervisor and digital machines used in cloud carriers may additionally have vulnerabilities, as exemplified by means of [14]. Such vulnerabilities represent a fair extra serious hassle in multi-tenant environments, wherein compromise of even a single digital system can have an effect on all users at the same physical server.

Virtualization is one of the foremost components of a cloud. However, this poses essential protection dangers. Ensuring that exceptional instances walking on the same physical device are remoted from each other is a primary assignment of virtualization which isn't met completely in nowadays state of affairs. The opposite difficulty is the control of administrator on host and visitor running structures. Contemporary virtual Machine monitor (VMMs do not provide the best isolation. Many bugs had been determined in all popular VMMs that permit escaping from VM. Virtual system monitor should be 'root relaxed', meaning that no privilege within the virtualized visitor environment lets in interference with the host machine.

Some vulnerability has been discovered in all virtualization software program which can be exploited by way of malicious, nearby customers to skip positive security regulations or gain privileges. As an instance, the vulnerability of Microsoft virtual server and Microsoft Virtual laptop ought to allow a guest operating system consumer to run code at the host or some other guest operating system. Vulnerability in virtual computer and virtual Server could allow elevation of privilege. Cloud vendors, consequently, would possibly need to reconsider conventional security issues from one of a kind angles.

III. CHALLENGES RELATED TO CLOUD SECURITY

Information Security

In a conventional on-premise software deployment version, the sensitive data of every organization keeps to live in the agency boundary and is a problem to its physical, logical and employees security and access management policies. however, inside the SaaS model, the business enterprise facts are saved outside the organization boundary, at the SaaS vendor cease. consequently, the SaaS seller must undertake extra protection exams to make sure statistics security and save you breaches due to safety vulnerabilities in the utility or through malicious personnel. This includes the use of robust encryption techniques for statistics safety and first-rate-grained authorization to govern get entry to data.

In cloud carriers together with Amazon, the Elastic Compute Cloud (EC2) administrators do now not have to get right of entry to patron times and cannot log into the guest OS. EC2 directors with an enterprise need are required to apply their character cryptographically robust relaxed Shell (SSH) keys to advantage get entry to a number [12]. All such accesses are logged and automatically audited. while the information at rest in simple garage service (S3) isn't always encrypted by default, users can encrypt their facts before it's far uploaded to Amazon S3, so that it is not accessed or tampered with through any unauthorized entity. Malicious users can make the most weaknesses of the statistics security model to gain

Security of the Network

In a SaaS deployment version, touchy information is obtained from the companies, processed by way of the SaaS utility and saved on the SaaS dealer stop. All records waft over the community wishes to be secured so as to prevent leakage of sensitive statistics. This involves the use of robust community traffic encryption techniques along with Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for safety.

In case of Amazon net services (AWS), the network layer presents tremendous protection against traditional network security problems, inclusive of man-in-the-middle attacks, IP spoofing, port scanning, packet sniffing, and so forth. for max protection, Amazon S3 is accessible thru SSL encrypted endpoints. The encrypted give up factors are reachable from each the net and from within AmazonEC2, ensuring that information is transferred securely both inside AWS and to and from sources outside of AWS [1]. but, malicious users can take advantage of weaknesses in network security configuration to sniff network packets.

Resource Locality

In a SaaS model of a cloud environment, the services supplied by the of the cloud companies used by the users without knowing precisely where the assets for such offerings are located, probably in different legislative domain names. This poses an ability problem whilst disputes appear, that's occasionally past the control of cloud providers. because of compliance and records privacy laws in various nations, locality of data is of utmost importance in plenty corporation structure [4]. The directive prohibits transfers of private records to countries which do now not make sure an adequate stage of protection. for instance, the recent Dropbox users ought to conform to the ‘‘terms of provider’’ which furnish the providers the proper to reveal person statistics in compliance with laws and law enforcement requests [2]. in addition to the problem of nearby laws, there’s additionally the query of beneath whose jurisdiction the information falls, when a research happens. A comfortable SaaS version ought to be capable of providing reliability to the client in the region of the records of the customer.

Standards of Cloud

To acquire interoperability among clouds and to growth their stability and security, cloud requirements are wished across extraordinary standard developing companies. for instance, the modern-day storage offerings through a cloud issuer may be incompatible with those of different issuer. to be able to keep their customers, cloud carriers can also introduce so known as ‘‘sticky offerings’’ which create an issue for the users if they need emigrate from one provider to the other, e.g., Amazon’s S3 is incompatible with IBM’s Blue Cloud or Google garage. There are currently a big variety of requirements our bodies with unique interests, e.g. IEEE Cloud Computing standard study group [14], ITU Cloud Computing focus organization Cloud security Alliance (CSA), distributed management assignment pressure], storage Networking enterprise affiliation, Open Grid Forum Open Cloud Consortium and so forth. To promote the wide use of cloud computing, those requirements bodies want to sit down and work collectively to set up commonplace standards. Feasible ‘‘Inter-cloud’’ standards inside the following domains are had to boom cloud interoperability and unfastened facts movement among clouds:

- ✓ Network architecture ,
- ✓ data format,
- ✓ Metering and billing,
- ✓ Quality of service

As stated, there are numerous general computing standards that can be reused inside the cloud, however, for the moment, there are to our information no dedicated cloud standards. this can upload to the confusion for cloud users [5], and is something which must be addressed in the future.

Data Segregation

Multi-tenancy is one of the main traits of cloud computing, due to multitenancy, the applications furnished via SaaS provides multiple users to store their data and data of diverse customers will reside at the identical location. The intrusion of information of one user via any other will become possible in this environment. This intrusion may be completed both via hacking via the loopholes inside the software or through injecting patron code into the SaaS system. A customer can write a masked code and inject into the utility. If the application executes this code without verification, then there is an excess capacity of

intrusion into differing's facts. A SaaS version has to, therefore, make certain a clear boundary for each users data. The boundary must be ensured at both the physical and application level. The service has to be smart sufficient to segregate the data belonging to various users of the cloud. A malicious user can use application vulnerabilities at handcraft parameters that bypass safety assessments and get admission to sensitive information of different tenants.

Data Access

Accessing data is an issue mainly associated with safety policies supplied to the customers at the same time as accessing the facts. In a regular situation, a small commercial enterprise can use a cloud supplied by using a few different company for carrying out its commercial enterprise methods. This organization may have its personal security regulations based on which every employee can have get admission to a particular set of information. the security regulations may additionally entitle a few concerns, in which, some of the employees are not given get entry to the sure amount of records [10]. these protection rules ought to be adhered through the cloud to keep away from the intrusion of facts via unauthorized customers [12].The SaaS model needs to be bendy enough to incorporate the specific guidelines put forward by using the agency. The version needs to also be capable of providing organizational boundary in the cloud because more than one organization may be deploying their enterprise approaches within a single cloud environment.

Web application security

Is software deployed over the internet and/or is deployed to run behind a firewall in local area network or personal computer. The key characteristics include Network-based access to, and management of, commercially available software and managing activities from central locations rather than at each customer's site, enabling customers to access application remotely via the Web. SaaS application development may use various types of software SaaS is software program deployed over the net and/or is deployed to run at the back of a firewall in the nearby region community or non-public laptop. the important thing traits include network-based totally get entry to, and management of, commercially available software and dealing with activities from critical locations in preference to at each client's site, enabling customers to access software remotely through the web.

SaaS software development may also use various sorts of software program additives and frameworks. those tools can lessen time-to-market and the value of converting a conventional on-premise software program product or constructing and deploying a brand new SaaS solution. Examples consist of components and frameworks. These tools can reduce time-to-market and the cost of converting a traditional on-premise software product or building and deploying a new SaaS solution. Examples include subscription management, grid computing software, web application frameworks, and whole SaaS platform products. one of the ''need-to-have'' requirements for a SaaS software is that it has for use and controlled by the web [8].

The software that is supplied as a service is living in the cloud without tying up with the actual customers. This allows improvising the software without inconveniencing the person. safety holes inside the net packages, as a result, create a vulnerability to the SaaS utility [9]. in this situation, the vulnerability can potentially have an unfavourable effect on all of the customers the usage of the cloud. The venture with SaaS protection is not any exclusive than with that of every other web application era. However one of the problems is that conventional network protection answers inclusive of network firewalls, community intrusion detection and prevention structures (IDS & IPS), do not effectively address this trouble. internet packages introduce new security dangers that can't successfully be defended in opposition to at the community stage and do require utility stage defences. The Open web application security venture [4] has furnished the ten most vital web applications safety threats.

Data breaches

considering data from diverse customers and commercial enterprise corporations lie together in a cloud environment, breaching in the cloud, surroundings will doubtlessly attack the information of all of the users. as a result, the cloud turns into a high-value goal [7]. within the Verizon enterprise breach record weblog it has been said that outside criminals pose the finest threat (73 percent), however, attain the least effect (30,000 compromised facts), ensuing in a Virtualization vulnerability [9].

Backup

The conventional backup strategies used within advance applications and records facilities that have been generally designed for net and client applications, aren't optimally designed for the packages strolling in the cloud. The SaaS dealer desires to make sure that each one sensitive agency statistics is often subsidized as much as facilitate quick healing in case of screw ups. and the use of robust encryption schemes to guard the backup facts is suggested to save you unintentional leakage of sensitive records. in the case of cloud companies such as Amazon, the facts at rest in S3 is not encrypted by means of default. The users need to one at a time encrypt their facts and backups in order that it cannot be accessed or tampered with via unauthorized parties.

Identity management and sign on process:

Identity management (IDM) or identity management is an area that deals with identifying individuals in a machine and controlling the access to the resources in that system by means of putting regulations on the established identities. This region is taken into consideration as one of the biggest challenges in statistics protection. while a SaaS company has to recognize the way to manipulate who has access to what structures inside the organization it will become all of the extra challenging challenges. In such eventualities, the provisioning and de-provisioning of the customers within the cloud will become very important.

IV. CURRENT SECURITY SOLUTIONS

The Cloud Security Alliance(CSA) permits and business enterprise to submit their security answers and standards for the cloud and gives a few requirements which need to be accompanied by the aid of the Cloud surroundings offering groups which is not a smooth project to build a hard safety architecture.

The Open Web Application Project (OWASP) maintains a list of pinnacle vulnerabilities to cloud-primarily based or SaaS fashions that are up to date because of the hazard landscape modifications . The Open Grid discussion board publishes files to containing security and infrastructural specifications and records for grid computing developers and researchers . Tsai W, positioned forth a 4-tier framework for web-primarily based improvement that although appears interesting best implies a protection side in the system. In his work, Berre has cautioned a street map in the direction of cloud-centric improvement, and the X10 language is one of the ways to acquire better use of cloud capabilities of big parallel processing and concurrency another approach is aid isolation to ensure the protection of facts at some stage in processing, through separating the processor caches in digital machines, and keeping apart the ones digital caches from the hypervisor cache. One simple answer, for UK organizations, is to in reality use in-house ‘‘non-public clouds’’ .Pearson highlighted that the contemporary loss of transparency is stopping many users.

V. CONCLUSION

Despite the fact that cloud –based system gives numerous advantages, there are yet many realistic troubles which need to be taken care of. Cloud computing is a disruptive generation with profound implications not handiest for Internet offerings however also for the IT sector as an entire. nonetheless, numerous extraordinary problems exist, particularly associated with service level agreement (SLA), security and privacy, and speed. As described in the paper, several customers will be scared to use cloud computing because of security loopholes. Till a proper safety module is not implemented in the cloud, the users will no longer be capable of leveraging the actual blessings of this technology.

This security module want to cater to all of them problems arising from all hints of the cloud. Every detail in the cloud need to be analyzed at each the macro and micro diploma and in the long run on the integrated solution needs to be designed and deployed in the cloud to draw and keep the capability consumers, until then, cloud surroundings will continue to be cloudy. In a cloud, wherein there are heterogeneous structures having a model in their asset fee, a single protection machine might be too expensive for nice applications and if there can be plenty less protection then the vulnerability aspect of some packages like economic and military programs will shoot up. On the other aspect, if the cloud has a common safety method in place, it's going to probably be an immoderate price asset target for hackers due to the reality that hacking the protection gadget will make the entire cloud vulnerable to attack.

On this paper a top degree view of the cloud computing carrier shipping model, SaaS alongside the Safety

demanding situations, including each the conventional and cloud unique safety challenges, associated with the model has been supplied quite a variety of recent dreadful conditions this is inherently linked to the modern-day cloud paradigm has also been deliberated within the paper. Storing data in cloud the environment is a large challenge which prevents many customers from using the Cloud, a realistic approach to offer protection and privacy for data, whilst it's miles located in a public cloud, changed into additionally referred to in this paper. The need for in addition work on various safety mechanisms has additionally been highlighted, that allows you to offer transparent services that can be depended on via all users.

VI. REFERENCES

[1]. Pratap Murukutla, K.C. Shet (2012).Single Sign On for Cloud .In: International Conference on Computing Sciences,2012 IEEE DOI 10.1109/ICCS.2012.66

[2]. Choudhary V.(2007). Software as a service: implications for investment in software development. In: International conference on system sciences, 2007, p. 209.

[3]. Amlan Jyoti Choudhury, Pardeep Kumar,Mangal Sain, Hyotaek Lim, Hoon Jae-Lee(2011).A Strong User Authentication Framework for Cloud Computing.In: IEEE Asia -Pacific Services Computing Conference,2011 IEEE DOI 10.1109/APSCC.2011.14

[4]. Cloud Security Alliance. Security Guidance for critical areas of focus in cloud computing Version 2.1.(2009) , (http://www.cloudsecurityalliace.org/guidance/csaguide.pdf).

[5]. Cloud Security Alliance. Security best practices for cloud computing,2010b [Accessed :July 2012].

[6]. Cloud Security Alliance. Guidance for identity & accessmanagement V2.1,2010a [Accessed :July 2012]. International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013 10

[7]. Heiser J.(2009) What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345. [2] Seccombe A.., Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, (2009). Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 25 p.

[8]. Softlayer. Service Level Agreement and Master Service Agreement,2009 /http:// www.softlayer.com/sla.htmlS [Accessed: October2012].

[9]. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800– 145, Gaithersburg, MD

[10]. European Union. Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 1995.

[11]. ITU,2013. Cloud Computing Focus Group. .[Accessed : January 2013]

[12]. SNIA.(2013).Storage Networking Industry Association. .[Accessed : January 2013]

[13]. DTMF,2013.Distributed Management Task Force. .[Accessed : January 2013]

[14]. IEEE CCSSG. IEEE Cloud Computing Standard Study Group. .[Accessed : January 2013]