IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 10, October 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

Cloud Security : Challenges and Concerns

Sahreen Sajad[1], Dr. Nagaraj Cholli[2]

Student, Dept. of Information Science Engineering, R.V. College of Engineering, Bengaluru, India[1]

Associate Professor, Dept. of Information Science Engineering, R.V. College of Engineering, Bengaluru, India[2]

ABSTRACT: Cloud Computing is an inextricable service in use that has become an essential part of technology. The facility is used in industrial as well as academic fields. As such, the security concerns posed to our data whether deletion, theft or leakage is a growing concern that needs an extensive research for us to deal with it. The data is highly susceptible to attacks and needs a proper research on the type of concerns our data is susceptible to. In this paper, we provide a detailed analysis on the cloud security and the concerns of the providers and the clients. This data can be used by researchers and technologists to know about various security threats and their effects. The data is provided with respect to different service models and additional security concerns. This paper aims to serve as a basis for engineers or technologists to provide solutions to the concerns raised here.

KEYWORDS: Cloud Computing, Cloud Security, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Shadow IT, Man-In-The-Middle Attack

I. INTRODUCTION

Cloud Computing or Internet Computing is the availability or delivery of services offered by a computer [28-32]. These include storage, servers, databases, and software. The technique lets users avail services on-demand rather than keeping the files or data in a local storage. Cloud Security is the protection of cloud computing services from theft, deletion or leakage. Often, techniques like firewalls, Virtual Private Networks (VPNs), and data encryption are used to provide the required cloud security. Cloud Security is necessary to protect our digital assets. Security concerns are posed to cloud from two point of views; security issues that are faced by cloud providers and those that are faced by cloud users. The data is stored with a third-party. Thus, the control on data is limited. The biggest risk faced related to cloud computing is cloud data security [20-27]. These include issues like confidentiality, access controllability, and integrity. Cloud providers face issues differently with respect to the three different cloud service models. These include Infrastructure as a Service (IaaS), Platform as a Service (Paas), and Software as a Service (Saas). Infrastructure as a service includes hardware that is managed over the internet e.g. Amazon Web Services. Platform as a Service include hardware as well as software tools managed over the internet e.g. Google app engine. Software as a Service are on-demand services hosted by a cloud service provider e.g. Google Apps[33-37]. With respect to the different models of cloud computing services, challenges faced are different. These challenges come under the category of concerns faced by the cloud computing providers. The security issues that the customers face is concerned with whether the company hosts the application or if the data is stored on the cloud.

II. LITERATURE SURVEY

A number of papers have been written that survey the various cloud security issues.
Authors in [1] discussed two computing paradigms - Service-Oriented Computing and Grid computing, and then proceeded to identify Cloud Computing challenges highlighting Cloud interoperability issue.
Authors in [2] addressed the challenge of making an effective controller. This control acts as a customer add-on beside the cloud utility service.
Authors in [3] survey cloud computing and highlight various architectural principles, state-of-the-art implementation as well as research challenges.
Authors in [4] address issues related to security and privacy in cloud computing. Besides, there is also a survey on resource allocation, load balancing, data management, data availability, scalability, compatibility and interoperability.
Authors in [5] address security issues. The idea of handing over important data to another company is detailed to understand data breaches and risks.
Authors in [6] pay a detailed attention to load balancing and suggest various algorithms and mechanisms to tackle the cloud computing security issues.
Authors in [7] point to the fact that data owners and data servers have different business interests. They recommend an auditing service that is independent and is correctly hostel on the cloud.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

III. CLOUD SECURITY ISSUES

1. Infrastructure as a Service Issues

Infrastructure as a Service includes hardware that is managed over the internet. The most common example of the model is Amazon Web Services. AWS provides on-demand platforms for cloud computing and APIs to its customers who include individuals, companies, and the government. The most concerning issue present in IaaS is Shadow IT. Shadow IT is also called Fake IT, Stealth IT or Embedded IT. This means that there can be usage of software and devices without an explicit approval from the IT department. In simple words, there are accounts that are being made created which are outside of IT visibility. The main cause of Shadow IT is the practice of companies to hire IT engineers or purchase some application without a full-fledged knowledge or proper supervision. These result in wasted investments, time wastage, inconsistent approach and business logic, enhancement barriers.

The most common example of Shadow IT is the circulation of unofficial data in USB flash drives or online e-mail services. Shadow IT further poses problems like data loss, cost issues, inefficiencies in the system, non-compliance, control and visibility loss. When a person who owns some piece of information leaves the company, data is immediately lost. For example, if a user account is terminated; all the customer information will be gone. If someone stops paying the bills, it could also lead to the same issue. The costs incurred are often unjustified because of Shadow IT as the scaling of the resources is incorrect. Cloud storage often witnesses the cost issues. Since, the data flow is uninformed, the capacity and security is difficult to plan in case of Shadow IT[8]. The consequences of Shadow IT are far worse for organizations which have strict compliance regulations. There is also a never-ending susceptibility to organizational attacks. Since data lies outside the scope of the organization, weak credentials are often victims of attack. Besides, the evident Shadow IT Risks, there isn't a full control on who can access the data. Malicious actors can easily steal the data which is hosted in a particular cloud infrastructure. These often takeover computer resources for benefits like crypto currency generation. These resources are then re-used to attack the infrastructure of the cloud and other third parties. Often, there is also a complication of lack of staff that has the required skills to protect the cloud infrastructure. There is also not a full-fledged visibility of what data is stored in the cloud. Apart from malicious actors, a malicious insider threat or misuse of the confidential data is also omnipresent. The security controls are not consistent over multi-cloud and on-premises environments. Multi-cloud refers to use of more than one cloud computing service present in one architecture. On-premises environments are deployed within the customer's IT infrastructure. These invite advanced attacks against the infrastructure of the cloud. Monitoring the workload systems also becomes difficult and challenging. One workload can also spread its attack to another workload. Thus, protecting data is a necessity for Infrastructure as a Service Model. As long as the customer becomes dependent on the applications and operating systems, more threats can emerge. The center of attack becomes the emerging new attacks that exist beyond just the data. It is necessary to exactly determine who can access the data and to track any modifications made to the resources. Abnormal behaviors need to be kept into check. A vast network analysis of traffic on the services is necessary.

2. Software as a Service Issues

Software as a Service are on-demand services hosted by a cloud service provider e.g. Google Apps. The Google Workspace is a collection of tools, products, software, and cloud computing services offered by Google. There are 131 Google Apps currently offered over a variety of platforms. The main issue faced because of Software as a Service Model revolves around data and access. This is because data and access are two sole responsibilities for the SaaS customers. There also some common issues as faced in the Infrastructure as a Service Model. These include Shadow IT, theft, lack of staff[9].What exact data is stored in the cloud is unknown. A malicious actor can also steal data in this model. Consider a customer escaping a virtual machine, but once inside a hypervisor, the attacker can modify code and steal data or install malware on the hardware devices. Besides, there is also an incomplete control over insensitive data. Insensitive data is the kind of data which can incur a huge loss or an advantage to others if disclosed or brought to others. Whatever data is transmitted to and from cloud applications is not completely monitored. The never ending risk of the cloud applications being provisioned outside of the visibility is also there.

The cloud application provider also faces advances threats and attacks. The cloud provider's operations are difficult to assess. Regulatory compliance is also not always maintained well. Regulatory compliance is an organization's set out goals or policies that are in accordance with the laws and regulations. Insider threats are also omnipresent as these have direct access to the hardware infrastructure and the networks. These privileged insiders have an advantage of having easily accessible systems[10].Another method of gaining access is by breaking authentication. Because there is an access to the accounts used to provision virtual, the attacker is thus able to use the cloud service's API or user interface to get rid of services or grant additional access if they wish. Installing a key logger on an administrator's desktop is a common method to access credentials of the cloud service. One more method of gaining access besides breaking

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

authentication is breaking encryption. The most common way to break encryption is to break the PKI. PKI or Public Key Infrastructure are the policies that govern the digital certificates and encryption.
A PKI generally provides a decent level of security against attackers[11]. However, browsers are built to trust a hundred different root-level certificate authorities which are present in different countries. Any of these certificate authorities can create a certificate for any user and help the attacker. Considering that an attacker manages to get a certificate from any certificate authority, they can easily create new certificates and perform man-in-the-middle-attack with ease. A man-in-the-middle attack (MITM) is an eavesdropping attack. The attacker sits in the middle and interrupts an existing conversation between two parties and quotes different cryptographic parameters with the client and the server for their own benefits.

3. Platform as a Service Issues

Platform as a Service include hardware as well as software tools managed over the internet e.g. Google App Engine. Google App Engine is a platform that lets applications function over its infrastructure. Thus, companies can build and run their applications without the need of an infrastructure[12]. PaaS Model is centered on shared resources. It is due to this reason that security concerns are because of critical information which can cause a data breach. If the customers have Administrator or shell access authorized, further security issues can occur if the attackers somehow gain access to the resources and change configurations according to need. Self-service entitlements are offered by the PaaS platform which could pose another problem if not properly configured. To avoid all these risks, providers need to be careful and use the best industry approved practices beside lay down clear policies and guidelines that govern the system. Interoperability is major risk posed. Interoperability can be defined as the ability of different cloud systems to communicate to each other. We might as well say that it is a code that works on different cloud providers simultaneously. Applications which are built to use specific vendors PaaS will mean that changes are to be made to use the similar services which are present on Platform-As-a-Service of another vendor. Host Vulnerability and Object Vulnerability are another two threats. Multi-user hosts can be used for multi-tenancy. In such an environment, the host is susceptible to attacks. In case of a breach, attacker will get direct access to the resources of the host and confidential data. Thus, provider needs to keep the security measures in check. Since, service providers can access and modify objects, a provider may grant access of on object to any user that is residing on the host. This type of an attack is completely unavoidable. Users may also mutually attack each other's objects since they are customers of the same host and the host lets them share the same set of resources. An outside third party can also directly attack a user object. Network communications need to be secured and access to any remote entity has to be controlled. Phishing attack, impersonation of another user, brute force attacks, and password-reset attacks can also occur. Encapsulation and Policy Enforcement Points are usually implemented for protection against the attacks.

At the time of authentication, a user reveals substantial amount of information. Proxy certificates can be used to reduce the associated risks. Thus, applications need to be protected from common and unexpected attacks. A real-time protection is the best solution. User accounts and app resources need to be protected. Security vulnerabilities need to be looked for by scanning applications. Testing and fixing dependency security issues is necessary. Penetration testing and threat modeling is also done. Activities and files have to be monitored. Code should be secure and data should be validated. Multi-factor authentication should be enforced. A strong password policy can also be implemented. Hence, the biggest challenge faced is the lack of visibility or control[13]. The popularity of cloud computing comes from the fact that the customer does not need to manage their resources. However, this poses the problem of less visibility and control over the asset of the customer since the responsibility is handed over. This impairs the organization vastly.The organization is now unable to verify the scale and efficiency of their security methods because of lack of visibility present in the tools and data used in the cloud platform. Since there is no complete control over assets, the response plans are usually incident. Due to these reasons, it becomes necessary for the organization to analyze the data and user to witness any abnormal behavioral patterns. Thus, it becomes necessary for the organization to be sure about which data should be accessible, how to track it and what sort of security controls need to be provided to prevent data breaches. The second biggest security challenge is the inability of some cloud platforms to comply with the industry regulations. Some of these include PCI DSS, GDPR, FISMA. Fines and penalties may have to be paid if the standard set by the industry regulations are not met. The solution is definitely checking with the service provider if they meet the regulations and checking with the suitable agencies if the provider is listed as a compliant. The failure of either can incur huge losses to the company financially as well as in terms of credibility. Data privacy issues are another big concern. A data breach can get the identities of customers stolen as well as bank accounts being drained. The company can thus result in a state of millions of fines and lawsuits that seek damages. If there is no proper cloud security, insensitive data present on the cloud is highly dangerous. Even if the cyber security present is strong, moving insensitive data can lead to violation of agreements between customers and the companies. Another major problem is that if the data has been breached, the customers are not always notified of it. Because of lack of visibility and control it

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

is almost impossible to identify what data has been compromised. And which resources have been affected. In the wort case scenario, it might be better to notify everyone present on the cloud service of the data breach. User Access Control is another challenge mentioned. This is one challenge that is nearly always the responsibility of the user. No matter which model is used, IaaS, PaaS, or SaaS, the user access control that comes along has to be checked. "Vendor Lock" is another concern. It is difficult to be restricted to a single security solution as it can be extremely limiting. The investment on security will also yield a poor return[14]. The vendor you're a customer of has no other competition. Whatever business you require, they will be your only choice if you do not want to start from scratch. Thus, while choosing the cloud service you must check the easiness in migrating the data from different services. To avoid vendor lock, a proper research before using a particular service is essential. Lack of personal experience in cloud security measures poses another threat. No matter what kind of production environment is needed, the right quality security experts have to be found. The problem becomes more challenging as not everyone is familiar with the accurate security solution depending upon the model used. Finding the right people can become extremely difficult. The apt solutions to deal with the problem are Managed Security Services. Managed Security Service Providers (MSSPs) are well-informed about a variety of tools and can form a team of experts for security problems. The security services can be conducted in-house or internally as per the agreements of outsourcing. The services include round-the-clock monitoring, management of firewalls, security assessments and responding to security emergencies. Six categories of functions can be listed out; these include on-site consultation, client network perimeter management, product resale, security monitoring, compliance monitoring, and penetration testing and vulnerability assessments. Companies like Accenture, Dell, IBM, Verizon, and Wipro provided Managed Security Services. A risk assessment needs to be run before adding a cloud service to an organization or for personal use. The risk assessment involves knowing the drawbacks and their impacts and how likely are the risks to occur. A document can be created that analyses the needs, issues, and threats and a solution can be found out accordingly. The appropriate solution can be found by knowing the exact security needs of the particular company.

IV. ADDITIONAL SECURITY ISSUES

1. Elasticity

Elasticity is the ability to adapt to changes in the workload such that the current demand is matched by the available resources. Hence, elasticity improves salability. This lets customers to scale up or scale down as per requirement. Scaling up and down means a user can get access to resources previously assigned to another user. This leads to major confidentiality issues as stated before. Besides, elasticity takes quite some time for the required virtual machine to be used. Thus, some important questions need to be asked before selecting a vendor. One needs to know if their vendors can dynamically auto-scale. It should also be known if traffic of other companies affects one's business. The vendor should be able to provide the required bandwidth requirements. A large customer onboarding the region should not affect one's business.

2. Multi-tenancy

As previously stated, Multi-tenancy provides offering services to multiple customers over a single instance of infrastructure. Since, resources are shared between tenants that reside on the same infrastructure; the confidentiality of data is compromised. Important information can leak and there can be a susceptibility of cyber-attacks.
Multi-user hosts can be used for multi-tenancy. In such an environment, the host is susceptible to attacks. In case of a breach, attacker will get direct access to the resources of the host and confidential data. Thus, provider needs to keep the security measures in check.

3. Insider and Outsider Attacks

A single management domain is responsible for the cloud. Thus, within an organization threats can occur. Cloud employees are hired with no particular standard in place. This lets third party vendors to easily access the data and sell it to some other organization or corrupt it. Outsider attack is an even bigger problem because it discloses the information to the public. Unlike private networks, clouds have many interfaces. Thus, hackers take an advantage of the situation and exploit the APIs.

4. Loss of Control and Data

A transparency model exists due to which organization remain unaware about location and data services. This lets the host offer services from anywhere in the world. Thus, organizations can lose data and they might not be even aware about the security mechanisms in place. In addition to this, data loss can incur economic and customer business loss. An important example of this is losing data without any proper backup.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

5. Network Security

Three major network security attacks include man-in-the-middle attack, port scanning and distributed denial of service attacks. As already stated, a man-in-the-middle attack (MITM) is an eavesdropping attack. The attacker sits in the middle and interrupts an existing conversation between two parties and quotes different cryptographic parameters with the client and the server for their own benefits. An IP Spoofing, ARP Spoofing or DNS Spoofing may take place. This stage is called the interception. After interception, decryption is done without alerting or notifying the user or application. This can be done by HTTPS Spoofing, SSL Beast, SSL Hijacking or SSL Stripping. HTTPS Spoofing lets the hacker send a fake certificate to the user's browser and holds a digital thumbprint. The attacker then gets access to any data entered by the victim. In SSL Beast, a malicious JavaScript infects the computer of the victim. This lets intercept encrypted cookies sent. SSL Hijacking lets the attacker pass fake authentication keys to the user as well as the application[15]. This appears to be a safe session but in reality the hacker has control to everything. SSL Stripping lets an HTTPS connection to downgrade to a HTTP connection. A secured connection is established with the application but an encrypted version is sent to the user. This lets the victim's whole session transparent to the hacker. To avoid Man-in-the-Middle Attacks, WiFi connections that do not have password protection should be avoided. If a browser notifies a website to be unsecured, proper actions should be taken. One should immediately log out of an application when its not in use. While carrying out sensitive transactions, public networks shouldn't be used. A notable incident of the attack was made by a Belkin wireless network router in 2003. It took control of the HTTP connection which was supposed to result in failure of the traffic to pass on to the destination. But instead, it responded as a server. Instead of displaying the page requested by the user, it displayed an advertisement of another product by Belkin. After a backlash from the technical users, the feature was removed from the router's firmware. In 2013, it was found that Nokia's Xpress Browser was decrypting HTTPS traffic on its proxy servers, giving the A distributed denial-of-service (DDoS) attack is an attempt for disrupting the usual traffic of some target server by increasing the requests with a flood of enormous Internet traffic. Interconnected machines and networks are used to carry out DDoS attacks. When a DDOs attack occurs, the site becomes unresponsive or abnormally slow. There is an unexplained surge in the requests for a page and the traffic originates from a single IP address. Some of the attacking techniques used to create DDoS Attacks include DDoS extortion, Challenge Collapsar Attack, Nuke, Peer-to-Peer attack. Often, a black hole route is created and traffic is funneled to that route. One can also limit the number of requests that a server can accept. Tools like Web Application Firewalls also assist in handling DDoS Attacks. The first DDoS Attack occurred in 1996. For several days, the services of Panix, an old Internet Service Provider were brought down. Cisco managed to figure out a proper defense against the DDoS attack. During the Honk Kong Protests in 2019, Telegram witnessed a DDoS attack which prevented the protestors to coordinate their movements. The Telegram founders claimed that the attack originated from IP addresses that were from China. Port Scanning is when a subscriber configures a group. It happens automatically when we configure the internet. The port allows exchange of information. Though the ports are not themselves sensitive to resources, but these need to be protected. While operating any hosted services, one should regularly check for their open ports. Since the number of open port is large, a simple script can be written that checks the vulnerability of the ports. Hackers tend to use this technique of port scanning to find out weak points in the victim's network. When hackers send messages to the port, a response is received. This response lets the attacker figure out if a port is in use or not. The various Port Scanning Techniques include Ping Scans, Vanilla Scans, SYN Scan, FTP Bounce Scan, and Sweep Scan. Ping Scan is the simplest port scanning technique. ICMP requests are sent to a number of servers in search of a response[16]. A Ping Scan be very well avoided using a firewall. Vanilla Scan is also a basic scanning technique. It attempts to connect to all 65,536 ports, all at a time. This can also be very well avoided using firewalls. A SYN Scan sends a SYN to the target, waiting for an acknowledgement. No response means no TCP connection is established. But the hacker comes to know if the port is open or not. An FTP Bounce Scan lets the hacker disguise their location. A Sweep Scan sends traffic to a number of computer ports and identifies the active ports. Though no information regarding any port activity is revealed, the hacker is informed whether the system is in use or not.

6. Malware Injection Attack Problem

Cloud computing witnesses data transfer between providers and consumers. This results in a requirement of authorization and authentication. During the data transfer, an attacker can very well insert malicious code. This means that the victim will have to wait for a job to be completed which was originally initiated by the hacker. Malware Injection Attacks can occur in IaaS, Saas, or PaaS. The two most common Malware Injection Attacks in Cloud Computing are the SQL Injection Attack and Cross Site Scripting (XSS) Attack. Besides these, the wrapping attack also occurs. SQL Injection Attack targets vulnerable databases present on SQL servers. A malicious code is inserted from there. If the attack is successful, the contents of the SQL can also be manipulated and any confidential data will be revealed. Criminal activities can also occur. Thus, the main consequences of an SQL Injection attack loss of confidential information, authentication and authorization errors, and data integrity issues. In Cross Site Scripting (XSS), malicious scripts like JavaScript, VBScript, HTML, and Flash are injected in the victim's web browser. The

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

cookie used for authorization is then used by the hacker to gain access to the session. This helps the attacker to access the account of the victim or fool the victim into clicking a malicious link. Wrapping Attack uses Extensible Markup Language (XML). A fake element which is known as a wrapper is embedded inside a message structure and then replaces the original content with a malicious code. Then, the code is sent to the server of the cloud computing infrastructure. The message body seeming to be authentic will allow the server to accept the bogus content[17]. This will result in the hacker gaining an access to confidential resources and data. Amazon's Elastic Compute Cloud (EC2) is susceptible to wrapping attacks. This was discovered in 2008.

7. Flooding Attack Problem

Using cloud computing, a number of servers can establish a communication and transfer data. Before processing the requests, authentication needs to be done first. This authorization requires CPU utilization and lots of memory. Because of an overloaded server, the data is transferred to another server. All the activities result in a flooded system which is being interrupted. Flood Attacks can also be classified as a type of DDoS attacks. It can also occur if a high volume of traffic is sent to the server which disables it to allow network traffic. Firewalls can help protect against a number of flood attacks. One of the most common types of flood attack is HTTP Flood Attack. It is based on client's request – GET Request and POST Request. GET Request retrieves image and text content. POST enables the user to send data to the server. Both POST and Get Methods can be used to initiate an HTTP Flood Attack but POST method is used more because of its ability to trigger complex server processing. A botnet increases the number of requests sent to the server. The attack is designed in a way such that server is forced to allocate maximum resources to each request. Under normal conditions, a server works this way as the traffic load is less. But in this case, the increased number of requests makes the page unresponsive or extremely slow. Often it is hard to decipher if the page is responsive because of an HTTP Flood Attack or because the page is genuinely visited by a lot of viewers. Firewalls can be used in this case to identify IP addresses that are sending a vast number of requests. A JavaScript Challenge can also be sent to the client to figure out if the client belongs to a botnet or a genuine user. The botnet's IP Address can also be blocked if the attacker's techniques are known. Usually, an HTTP Flood Attack can be stopped in a matter of just a few minutes if the strategy of the attacker is known. Though protecting oneself from HTTP flood attacks is difficult as these look like normal traffic to a page and no malware is sent to the victim, but captcha tests can be introduced to protect oneself from HTTP Flood Attacks. Botnets will fail the tests and their IP addresses can be then blocked[18].

V. CLOUD COMPUTING SECURITY STANDARDS

To implement proper security, some standards exist which have defined procedures and rules. These include Security Assertion Markup Language (SAML), Open Authentication (OAuth), OpenID, and SSL/TLS.

1. Security Assertion Markup Language

Security Assertion Markup Languages are used in business deals so that the communication between the client and the provider is secure. It is an XML-based markup language. There are three roles defined by SAML. These are the principal, the identity provider (IdP), and the service provider (SP). The principal is generally human. The principal is allowed to make requests from the service provider. The service provider, in turn, requests authentication from the identity provider. SAML was chartered in January, 2001 by The Oasis Security Services Technical Committee (SSTC). Four intellectual property documents were contributed. These included S2ML from Netegrity, AuthXML from Securant, X-TASS from VeriSign, and ITML from Jamcracker. These became a basis for SAML V1.0. Since the initial version, one minor and one major revision has occurred. It is built upon a number of existing standards. These include XML< XML Schema, XML Encryption, Hypertext Transfer Protocol, and SOAP. SAML lets user provides requests and responses. These are then used to specify authorization and authentication information in XML format. The party that raises queries is an online website that receives the required security information.

2. Open Authentication (OAuth)

Open Authentication is a standard laid for internet users to access different information on websites without giving out any passwords. This standard is used by big companies like Google, Amazon, Facebook, Twitter, and Microsoft. The users are allowed to share their data with third-party applications. OAuth started in November, 2006 when Twitter OpenID was being developed. A discussion group was created for interested parties and OAuth 1.0 protocol was published in April, 2010. A later version OAuth 2.0 was also developed.

3. OpenID

OpenID is an open standard protocol. It allows users to be authenticated by websites whch are relying parties usign a third-party service. It allows users to log on to multiple websites without having an identity and password for each.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

Over 1 billion OpenID accounts exist as of now. Websites like Google, Amazon, Myspace, WordPress, Yahoo, PayPal have integrated OpenID support. OpenID was created in 2005 by an open-source community. Thus, OpenID is decentralised and has no owner. Anyone in the world who wans to become a user of OpenID or become an OpenID Provider can do so. There is an end-user who wants to have a aparticular identity. An application is called a relying party that want to verify the user's identity. The communication betwween the two is facilitated by the OpenID. A program called the user-agent enables the communication between the two parties.

4. Transport Layer Security (TLS/SSL)

Transport Layer Security provides a secure, protected connection over TCP/IP. TLS was formerly known as Secure Sockets Layer (SSL). The protocol is widely used in e-mails and Voice over IP. A number of security measures are provided by TLS. It protects against downgrading of a protocol[19]. A sequence number is used to number application records. A message digest is sued which is enhanced using a key. The ending message sends a hash. The input data is split and processed with a hashing algorithm which helps in creating the MAC. A significant number of attacks can happen against TLS. These include renegotiation attack, FREAK attack, Logjam Attack, Down Attack, BEAST Attack, POODLE Attack, and SWEET32 Attack. Renegotiation attack allows the hacker to introduce its own requests in the beginning of the conversation. FREAK Attack and Logjam Attack are downgrade attacks. It tricks the serer into negotiations with previous versions of TLS. BEAST attack uses JAVA applet to violate the policies. Apple has fixed the BEAST vulnerability in TLS. SWEET32 Attack injects a malicious JavaScript code and breaks the ciphers.

VI. RESULTS

This paper explains challenges and concerns present in cloud computing security in detail. In the recent years, cloud computing has gained a wide popularity. Besides all the benefits that the cloud computing provides to an end-user, the experience can also come at costs if proper analysis is not done with respect to the security concerns. As such, this paper aims to tackle the said issues. In this paper, proper categories are built to classify the threats various agents provide to the cloud computing experience so as to deal with them efficiently. This research paper is written in hopes for technologists and engineers to identify cloud computing security concerns in detail with an aim to look up for solutions to be provided for a smooth experience to the end-users. The goal is to make the cloud computing experience better and less susceptible to attacks by hackers. This is in view of the fact that the cloud computing domain is very essential to users who cannot compromise with the confidentiality of their data or the data integrity.

We believe this paper will prove to be helpful to anyone who believes in a secure experience of cloud computing and wants to provide solutions to concerns and challenges that we all can become victims to at some point or the other. A subsequent work with respect to solutions of all the concerns mentioned can also be undertaken. That can serve as a basis for tools and technologies to be developed to make the cloud computing experience a safe and secure one.

REFERENCES

[1] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges," 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 27-33, doi: 10.1109/AINA.2010.187.

[2] Harold C. Lim, Shivnath Babu, Jeffrey S. Chase, and Sujay S. Parekh. 2009. Automated control in cloud computing: challenges and opportunities. In Proceedings of the 1st workshop on Automated control for datacenters and clouds (ACDC '09). Association for Computing Machinery, New York, NY, USA, 13–18. DOI:https://doi.org/10.1145/1555271.1555275

[3] Zhang, Q., Cheng, L. & Boutaba, R. Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1, 7–18 (2010). https://doi.org/10.1007/s13174-010-0007-6

[4] F. Fatemi Moghaddam, M. Ahmadi, S. Sarvari, M. Eslami and A. Golkar, "Cloud computing challenges and opportunities: A survey," 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), 2015, pp. 34-38, doi: 10.1109/TAFGEN.2015.7289571.

[5] Kuyoro, S. O. and Ibikunle, F. and Awodele, O. (2011) Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 3 (5). pp. 247-255.

[6] K. A. Nuaimi, N. Mohamed, M. A. Nuaimi and J. Al-Jaroodi, "A Survey of Load Balancing in Cloud Computing: Challenges and Algorithms," 2012 Second Symposium on Network Cloud Computing and Applications, 2012, pp. 137-142, doi: 10.1109/NCCA.2012.29.

[7] Yang, K., Jia, X. Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web 15, 409–428 (2012). https://doi.org/10.1007/s11280-011-0138-0

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

[8] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," 2011 World Congress on Information and Communication Technologies, 2011, pp. 217-222, doi: 10.1109/WICT.2011.6141247.
[9] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.
[10] V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.
[11] M. Jensen, N. Gruschka, and R. Herkenh¨oner, "A survey of attacks on web services", Computer Science Research and Development (CSRD), Springer Berlin/Heidelberg. 2009.
[12] M. A. Vouk, "Cloud computing - Issues, research and implementations," Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.
[13] Kuyoro S. O., Ibikunle F. & Awodele O; Cloud Computing Security Issues and Challenges; International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011; pp 247-257.
[14] P.Buddha Reddy, Vinod Bhupathi, and Ch Sravan, "Survey on Security Issues in Platform-as-a-Service Model" International Journal of Computer Science and Mobile Computing, vol. 6, issue 4, April 2017.
[15] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010
[16] Subashini, S. & Kavitha, V.. (2011). Kavitha, V.: A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Application 34(1), 1-11. Journal of Network and Computer Applications. 34. 1-11. 10.1016/j.jnca.2010.07.006
[17] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010
[18] "Krešimir Popović, Željko Hocenski,"Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia
[19] Nagarjuna,C.C kalyan srinivas,S.Sajida,Lokesh" SECURITY TECHNIQUES FOR MULTITENANCY APPLICATIONS IN CLOUD", C.C. Kalyan Srinivas et al, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, August 2013
[20] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, "Secure Artificial Intelligence of Things for Implicit Group Recommendations", IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.
[21] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, F. A. Khan, "Securing Critical Infrastructures: Deep Learning-based Threat Detection in the IIoT", IEEE Communications Magazine, 2021.
[22] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, "Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness", IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.
[23] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things", ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.
[24] Z. Guo, K. Yu, A. Jolfaei, A. K. Bashir, A. O. Almagrabi, and N. Kumar, "A Fuzzy Detection System for Rumors through Explainable Adaptive Learning", IEEE Transactions on Fuzzy Systems, doi: 10.1109/TFUZZ.2021.3052109.
[25] Yang, D., Karimi, H.R. and Sun, K., 2021. Residual wide-kernel deep convolutional auto-encoder for intelligent rotating machinery fault diagnosis with limited samples. Neural Networks, 141, pp.133-144.
[26] Lei, Y., Karimi, H.R., Cen, L., Chen, X. and Xie, Y., 2021. Processes soft modeling based on stacked autoencoders and wavelet extreme learning machine for aluminum plant-wide application. Control Engineering Practice, 108, p.104706.
[27] Havedanloo, S. and Karimi, H.R., 2013. Improving the performance metric of wireless sensor networks with clustering Markov chain model and multilevel fusion. Mathematical Problems in Engineering, 2013.
[28] Hu, L., Nguyen, N.T., Tao, W., Leu, M.C., Liu, X.F., Shahriar, M.R. and Al Sunny, S.N., 2018. Modeling of cloud-based digital twins for smart manufacturing with MT connect. Procedia manufacturing, 26, pp.1193-1203.
[29] Shahriar, M.R., Al Sunny, S.N., Liu, X., Leu, M.C., Hu, L. and Nguyen, N.T., 2018, June. MTComm based virtualization and integration of physical machine operations with digital-twins in cyber-physical manufacturing cloud. In 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 46-51). IEEE.
[30] Nguyen, T.N., Zeadally, S. and Vuduthala, A., 2021. Cyber-physical cloud manufacturing systems with digital-twins. IEEE Internet Computing.
[31] Do, D.T., Nguyen, T.T.T., Nguyen, T.N., Li, X. and Voznak, M., 2020. Uplink and downlink NOMA transmission using full-duplex UAV. IEEE Access, 8, pp.164347-164364.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010068 |

[32] Pham, N.V., Nguyen, T.N., Ngo, T.D., Truong, A.T. and Nguyen, G.L., 2021. A novel approach for pivot-based sensor fusion of small satellites. Physical Communication, 45, p.101261.

[33] Puttamadappa, C. and Parameshachari, B.D., 2019. Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique. Microprocessors and Microsystems, 71, p.102886.

[34] Subramani, P., Rajendran, G.B., Sengupta, J., Pérez de Prado, R. and Divakarachari, P.B., 2020. A block bi-diagonalization-based pre-coding for indoor multiple-input-multiple-output-visible light communication system. Energies, 13(13), p.3466.

[35] Kumar, M.K., Parameshachari, B.D., Prabu, S. and liberata Ullo, S., 2020, September. Comparative Analysis to Identify Efficient Technique for Interfacing BCI System. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012062). IOP Publishing.

[36] Shivappriya, S.N., Karthikeyan, S., Prabu, S., Pérez de Prado, R. and Parameshachari, B.D., 2020. A modified ABC-SQP-based combined approach for the optimization of a parallel hybrid electric vehicle. Energies, 13(17), p.4529.

[37] Shivappriya, S.N., Priyadarsini, M., Stateczny, A., Puttamadappa, C. and Parameshachari, B.D., 2021. Cascade object detection and remote sensing object detection method based on trainable activation function. Remote Sensing, 13(2), p.200.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details