ADDRESSING CLOUD COMPUTING SECURITY ISSUES WITH SOLUTIONS

Suvarchala Naidu
Department of Computer Science and Engineering
Oakland University
Rochester, MI, USA
suvarchalanaidu@oakland.edu

Mohammed Mahmoud
Department of Computer Science
Bemidji State University
Bemidji, MN, USA
prof.mahmoud@bemidjistate.edu

***Abstract*—The provision of IT resources on demand as opposed to the acquisition, ownership, and upkeep of physical servers and data centers is known as cloud computing. Recent cloud computing applications involve crucial infrastructure like power plants and distribution facilities. The majority of necessary services are outsourced, which puts data security and privacy at risk. This paper outlines potential security concerns and practical solutions. A brief explanation of cloud computing is provided prior to the analysis and examination of the security issues.**

Keywords—Information Technology (IT), cloud computing, security, privacy, solutions.

I. INTRODUCTION

Cloud computing is the delivery of computing service that includes servers, storage, databases, networking, software, analytics and intelligence-over the Internet to offer faster innovation, flexible resources, and economies of scale. Instead of having local servers or personal devices manage applications, cloud computing is a utility-driven, based on pay-as-you-go (PAYG) technology for remotely sharing the information technology (IT) resources [19]. It has different advantages over grid computers and other networking systems. Cloud computing is one of the new generations of structural processing, which creates a promising solution to manage explosive enrollment in a multi-faceted environment and information size. Clouds bring out a wide range of benefits including configurable computing resources, economic savings, and service flexibility [1]. The Cloud Service Provider (CSP) should ensure integrity, availability, privacy and confidentiality, but CSP faces many challenges in providing reliable data services to the customer [2].There are the three largest public CSPs that have established themselves as dominant fixtures in the industry – Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Cloud computing lowers the requirement for user engagement by hiding technical issues like software upgrades, licenses, and maintenance from its users, making many aspects like the location of the service, hardware, and operating system unimportant to the user. Additionally, compared to standalone server deployments, clouds may provide higher security benefits. The cloud has introduced new ideas like multi-tenancy, resource sharing, and outsourcing that provide new difficulties for the security industry. Due to the security and privacy concerns associated with the use of cloud computing services, the market size is currently far behind expectations even though cloud computing has several potential advantages when compared to the old IT paradigm.

II. CHARACTERISTICS OF CLOUD COMPUTING

A. Flexibility

Users can easily gain access to computational resources without any human contact. The provision of application programming interfaces (APIs) and other development tools for customizing services, access to data in real-time on their own mobile devices regardless of their location and allowing users to select the delivery model as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are some features enabling flexibility in cloud computing.

B. Scalability of infrastructure

The cloud architecture can be scaled up or down as needed. As long as the system is properly maintained, cloud computing offers rapid and simple resource assignment within a regulated environment, simulating the peak load without issue. The managed datacenters are a desirable business solution for small to large enterprises. This characteristic increases the adaptability of cloud computing.

C. Device and Location independence

Cloud services are not device-specific. Any computer with an internet connection can access them. The offered resource's precise location is unknown to the consumer, but they can be specified using a higher level of abstraction, such as a country or state. The virtualization system controls the process of mapping logical entities to the actual physical location and exposes them to the user as volumes.

D. On-demand self-service

It is based on a self-service approach, allowing customers to take control of their services by managing things like their allotted storage, features, server uptime, etc. This gives users the ability to be their own boss. Users can use the cloud site directly to pick and use the tools and resources they need while keeping track of their consumption. Users are made more responsible for their consumption and can make better judgments as a result. Depending on their needs and requirements, users can make use of resources. Users are only charged at the end of the billing cycle depending on their consumption of the services by the cloud service providers; they are not instructed on how to manage their services.

E. Virtualization

Virtualization enables the virtualization of all infrastructure services. Therefore, rather than keeping their own resource pool, users can access services via the web and obtain data from the cloud on a rental basis [13].

F. Maintenance

The upkeep of the cloud is a simple, automated procedure that requires little to no additional money. Upgrading cloud

979-8-3503-2028-2/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCI58124.2022.00293

software and infrastructure makes maintenance easier and more affordable.

G. *Automation*

IT teams and developers can create, change, and maintain cloud resources thanks to automation. Minimum human engagement is necessary for cloud infrastructure. Almost everything is automated, including configuration, maintenance, and monitoring. The quick spread of cloud services and the rise in demand are both largely due to automation, which is a great feature of cloud computing.

III. Service Models Provided by Cloud Computing

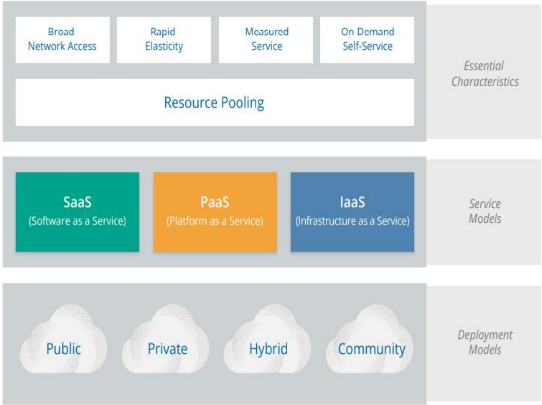

Fig. 1. Models and characteristics of cloud computing.

There are three basic services provided by cloud computing as shown in the figure below. These are sometimes referred to as "SPI" tiers.

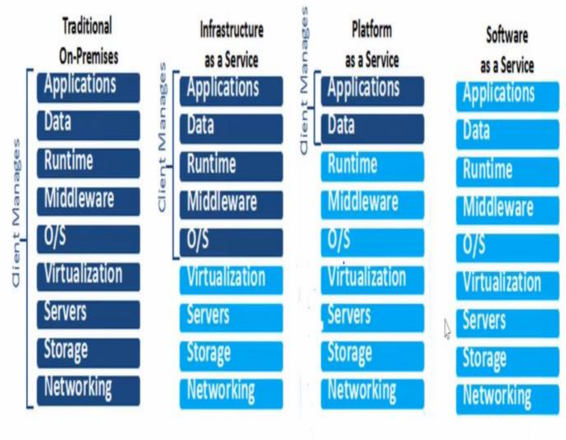

Fig. 2. Service models.

- *Infrastructure as a Service (IaaS):* In addition to supplying the necessary tools, the service provider is responsible for housing, operating, and maintaining the API as a service. Physical or virtual servers, storage, and networking are the three basic components of computing that can be hired under the term IaaS. This is alluring to businesses that want to create applications from the ground up and have almost complete control of the process themselves, but it does necessitate those businesses have the technical know-how necessary to coordinate services at that level [2].
- *Platform as a Service (PaaS):* This gives developers the freedom to create applications on the platform of the provider. The next layer up is called PaaS, and it includes virtual servers, storage, networking, middleware, database management, operating systems, and development tools, among other things. This layer also includes the software and tools that developers will need to build applications on top of it.
- *Software as a Service (SaaS):* It is the software that operates on the cloud infrastructure of the provider. The delivery of programs as a service is known as SaaS and is perhaps the aspect of cloud computing that most people are accustomed to on a daily basis. The end user, who will access the service through a web browser or app, is unconcerned about the underlying hardware and operating system; it is frequently purchased on a per-seat or per-user basis.

Security challenges exist with cloud service models also. The following table lists the security issues that pertain to each of these models [13].

TABLE I. Security Issues in Service models.

SaaS	▪ Privacy of data. ▪ Nnetwork security and locality. ▪ Integrity and access of data. ▪ Authentication. ▪ Backup. ▪ Availability.
IaaS	▪ Taking virtual machines off creates security challenges. ▪ Security issues in operating systems.
PaaS	▪ Apps are built by users and this control is given to them by the provider. Security of the apps is controlled by the provider only. ▪ If hackers can attack the infrastructure of an app, they are more likely to attack the visible code of it.

IV. Types of Cloud Computing

There are four different types of cloud computing models based on who owns the infrastructure. In a public cloud, resources are dynamically provided on a self-service basis over the Internet. A private cloud is more desirable due to the use of virtualization. A community cloud refers to shared infrastructure within a particular community. A hybrid cloud which as the name implies, is a combination of any two or all of the above models. In addition to these four, there is multicloud, where an organization uses a combination of clouds to distribute applications and services. These clouds can be two or more public clouds, two or more private clouds, or a combination of public, private and edge clouds.

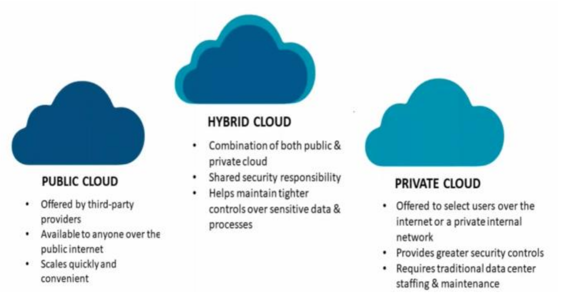
HYBRID CLOUD
• Combination of both public & private cloud
• Shared security responsibility
• Helps maintain tighter controls over sensitive data & processes
PUBLIC CLOUD
• Offered by third-party providers
• Available to anyone over the public internet
• Scales quickly and convenient
PRIVATE CLOUD
• Offered to select users over the internet or a private internal network
• Provides greater security controls
• Requires traditional data center staffing & maintenance

Fig. 3. Types of cloud computing.

V. Security Issues and Threats

Since a cloud pools resources, cloud providers hire specialized security personnel, as opposed to normal businesses, which may only have a network administrator who may not be knowledgeable about cyber security issues. Virtual Machines (VMs) that move from one physical machine to another can perform mobile computations thanks to the clouds. Mobile computations assist in avoiding environments where a single administrator has complete control over the calculation in addition to reducing the threat of targeted Distributed Denial of Service (DDoS) attacks.

A survey on cloud computing indicated that more than 70% of potential cloud users refuse to use cloud services because of security issues [19]. Accidents like the disclosure of user personal data due to flaws in Google Docs and the twice-involved outages of Amazon's Simple Storage Service in 2009 have emphasized the requirement for establishing the security and dependability of such systems. The new technology and services related to the cloud computing infrastructure have not been fully evaluated with respect to security. This section lists some security issues.

A. Trust

The major problem for all is a lack of trust between the serving and receiving ends. The Service Level Agreement (SLA) contract binds the service ends since the person on the receiving end can never be certain that the serving end is giving reliable data [9]. In the cloud computing context, the organization is in charge of the infrastructure. As security is related to trusting the procedures and computer infrastructure used by cloud owners, this poses a range of dangers and threats.

B. Missing Perimeter Security

A collection of physical and programmatic security standards known as perimeter security offer varying degrees of protection on the notional edge against remote hostile activity. In the cloud computing model, the boundary is hazy. From a typical perimeter security perspective, the cloud looks to be outside the trust threshold and should be looked at with skepticism, but this results in a lack of trust in crucial business operations and outsourced services.

C. Risk of Unauthorized Use

The possibility of unlawful usage of cloud services rises as a result of the lower costs and simplicity of installing PaaS and SaaS solutions. Unauthorized cloud service usage may lead to a rise in malware outbreaks or data espionage. Additionally, it runs the danger of reducing an organization's network, data visibility and management.

D. Internet-Accessible Management APIs can be Compromised

Customers can control and communicate with cloud services via a set of APIs that the cloud security providers disclose. APIs are frequently provided by CSPs to their clients. To make these interfaces simple for a CSP's clients to use, they are typically well-documented. However, if a customer has not adequately protected the interfaces for their cloud-based infrastructure, this could present problems. The software flaws in these APIs are identical to those in an operating system API. If the attackers are successful in exploiting a vulnerability, they may carry out additional attacks against other clients.

E. Data Confidentiality Issue

Both the cloud provider and other customers who are using the cloud infrastructure should maintain confidentiality as the cloud data is available publicly. It prevents disclosure of any private information [9].

F. Data Availablity Issue

The user will not have access to the data in the event of a cloud failure. Denial of Service (DoS) attacks and flooding attacks that result in service denial are threats to data availability. Different levels of on-demand service will be offered through cloud computing. Customers may lose trust in the cloud system if a specific service is discontinued, or the quality of service falls short of the SLA.

G. Potential Theft of Intellectual Property (IP)

Many businesses are quite concerned about IP theft. The World Intellectual Property Organization (WIPO) statistics indicate that more than 3.3 million patent applications were submitted in 2018 alone. These intellectual property rights give the companies that own them a competitive edge, thus their theft or loss can have a real effect on market shares because imitators can make goods and procedures for less money because they don't have to pay for research and development.

H. Misconfiguration

A major factor in cloud data breaches is incorrectly configured cloud security settings. Because enterprises frequently deploy many clouds, each with a unique set of vendor-provided security measures, it is simple for a setup error or security lapse to leave an organization's cloud-based resources vulnerable to attackers.

I. Traffic Hijacking

By allowing a single stolen password to be used on numerous distinct accounts, password reuse exacerbates the effects of weak passwords and data breaches. As enterprises increasingly rely on cloud-based infrastructure and applications for critical business processes, account hijacking is one of the more serious cloud security challenges.

J. Denial of Service (DoS)

Important internal and customer-facing applications are run on the cloud, which also stores data that is crucial to business operations. A variety of different businesses will be impacted if a DoS assault against cloud infrastructure is successful.

K. Malicious Insiders

Given their access and privileges, employees who commit malevolent acts within an organization have the potential to cause significant harm. This is made worse by the fact that such activity may take place both inside and outside of the client organization and the supplier organization in the cloud computing environment.

L. Insufficient Due Diligence

When the essential precautions are either insufficiently taken, or not taken at all, to ensure proper security and the credibility of the service provider, this is known as insufficient due diligence or lack of due diligence.

M. Data Breaches

A data breach occurs when sensitive information leaves your possession without your knowledge or permission. Other sensitive information, such as internal documents or emails, could be used to damage a company's reputation or sabotage its stock price. No matter the reason for stealing the data, breaches continue to be an imposing threat to companies using the cloud.

N. Management Interface Vulnerability.

Interfaces to manage public cloud resources (such as self-provisioning) are usually accessible through the Internet. Since they allow access to larger sets of resources than traditional hosting providers, they pose an increased risk, especially when combined with remote access and web browser vulnerabilities [3].

O. Hardware Level Vulnerabilities

Flaws at the hardware level that provide attackers access to the data of other residents, or potentially compromise the hypervisor. Like the other vulnerabilities, they can serve as grounds to create new attack vectors [16]. The IaaS service model is most susceptible to this threat. It is challenging to fix these vulnerabilities and doing so has an impact on the system's performance. Since these are the most recent risks, little study has been done to address how to reduce them in the context of cloud computing [17].

P. Virtual Machine or Hypervisor Attacks

A VM or hypervisor is compromised, giving hackers access to the hosts' operating system (OS). They have the ability to mishandle or steal data and apps when they control the VM. An example of this kind of attack is a zero-day attack [18].

VI. Attacks on Clouds

Being aware of the attacks and its effect landscape will help understand the pressing need to induce security in the cloud computing environment. This section lists ways to attack cloud computing services.

A. Account or Service Hijacking

Account or service hijacking is achieved after gaining access to a user's credentials. There are various techniques for achieving this, from fishing to spyware to cookie poisoning. Once a cloud account has been hacked, attackers can obtain a user's personal information or corporate data and compromise cloud computing services.

B. Side Channel Attack

It is arranged by hackers when they place a malicious virtual machine on the same host as the target virtual machine. During a side channel attack, hackers target system implementations of cryptographic algorithms.

C. Man-in-the-middle Attack

The man-in-the-middle attack refers to an attack in which an attacker is active in the middle and accesses the data that is passed between two parties. This attack is possible due to lack of security configuration in a Secure Socket Layer (SSL). The two parties, including providers communicate with each other in the cloud, at this time an attacker is residing in the middle and capable of accessing the data, if the communication channel is not secure [8].

D. Phishing Attack

Phishing attacks are performed by manipulating a web link. A legitimate user is redirected to a fake webpage, believing it is a secure page, and enters their credentials (user-name and password). After that, the attacker can access his credentials [8].

E. Advanced Persistent Threats (APTs)

APTs are attacks that let hackers continuously steal sensitive data stored in the cloud, or exploit cloud services without being noticed by legitimate users. The duration of these attacks allow hackers to adapt to security measures against them. Once unauthorized access is established, hackers can move through data center networks and use network traffic for their malicious activity.

F. Cloud Malware Injection Attacks

Malware injection attacks are done to take control of a user's information in the cloud. For this purpose, hackers add an infected service implementation module to a SaaS or PaaS solution, or a VM instance, to an IaaS solution. If the cloud system is successfully deceived, it will redirect the cloud user's requests to the hacker's module, initiating the execution of malicious code. Then the attacker can begin their malicious activity such as manipulating and stealing data, or eavesdropping [4].

G. Distributed Denial of Service (DDoS) Attacks

DDoS attacks affect all layers of the cloud system (IaaS, PaaS, and SaaS) and can occur internally or externally. An external cloud-based DDoS attack starts from outside the cloud environment and targets cloud-based services. This type of attack affects the availability of services. There are various types of DDoS attacks like IP flooding, Smurf attacks, Buffer overflow, Ping of Death, Land.c, Teardrop.c [7].

H. Cookie Poisoning Attacks

In this type of attack, the cookie's contents are modified to gain access to an unauthorized program or website. The cookie holds private information about users, and if a hacker is able to access these contents, he will also have access to the information contained therein and be able to commit crimes [15].

VII. Solutions for Security Issues

A. Addressing Trust Issue

Trust Issues can be addressed by the use of inter-cloud as there is a hierarchy of priority of cloud computing services. In inter-clouds we maintain remote data centers for providing services to end users, government authorities and companies [5].

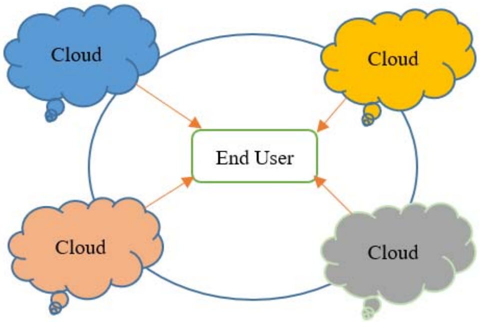

Fig. 4. Inter-clouds environment.

In inter-cloud environments as shown in Fig 4., an end user or a company will make requests to many cloud service providers. Though this model ensures service availability, there is a data intrusion threat still available. Below are a few techniques adopted to counter various security issues. The challenges in inter-clouds can be encountered by taking aid of any of the methods below.

B. *Addressing Data Availability Issue*

Cloud providers must provide a safe recovery facility to avoid data unavailability issue. A recovery facility enables the continuity of data if the data is lost. Data duplication, redundancy, backups and resilient systems can be used to address availability issues.

The data dispersion technique can be used to address the availability issue if other methods are not effective. Here the data is stored as fragments in many clouds and the data can be reconstructed when it is required from the fragments.

C. *Trusted Third Party*

There can be deployment of Trusted Third-Party Services to establish a necessary trust level and provide ideal solutions to preserve confidentiality, integrity and authenticity of data and communications [14].

The trusted third party can be relied upon for:
- Low- and High-level confidentiality.
- Server and Client Authentication.
- Creation of Security Domains.
- Cryptographic Separation of Data.
- Certificate-Based Authorization.

D. *Addressing Data Confidentiality Issue*

Though encryption cannot protect data against configuration errors and software bugs, it can avoid data confidentiality issue. Encryption is typically used by cloud system users to guarantee the security of their private data kept on the cloud server [19]. It should be applied when data is at rest, and when data is in transit. Sensitive data utilized by cloud-based VM should be encrypted, key management should be centralized so that users, not cloud providers, may govern cloud data, and cloud data should be made accessible in accordance with established corporate standards [20].

Image Steganography: This method of steganography is used to conceal information so a sent secret message is not discovered. The image is utilized as the cover information in image steganography. The cover photo is the one that contains the secret information [10]. Stego-image is the name given to the image created by encrypting the cover image with secret information. By utilizing a pixel key pattern to locate the image's edges, the secret data is implanted into the picture [12].

Pixel Key Pattern: Edge detection is a tool used in image processing and computer visualization. It is the process which aims at identifying and locating sharp points in an image which are due to a change in pixel intensity. The most common algorithm used for edge detection is the pixel key pattern. It uses a multistage algorithm to detect a wide range of edges in an image. The characteristics of this algorithm have a low error rate, and edge points are well localized [11].

E. *Addressing Data Integrity Issues*

Third Party Auditing (TPA) can be employed to check for data integrity. Many researchers insist to audit data integrity by third-party auditors because they are specialized in it.

F. *Addressing Risk of Unauthorized Use*

- Apply single-sign-on policy where ever possible.

- Multi-factor authentication can be employed which enables both identity and access management and it is used by Amazon Web Services (AWS).

- Biometric authentication has the potential to be the most secure form of single-sign-on authentication.

- Intrusion Detection System (IDS), firewalls as well as segregation of obligations can be implemented on the different network and cloud layers to enable proper access control in cloud computing for better data protection

- Cloud applications should use open standards where applicable, such as Security Assertion Markup Language (SAML), an XML-based Organization for the Advancement of Structured Information Standards (OASIS) an open standard for exchanging authentication and authorization data between security domains, and Open Authorization (OAuth) an open standard for authorization, allowing users to share their private resources using tokens rather than credentials.

- Check Access – Each use of a direct reference from an untrusted source must be checked for access control to ensure that the user is authorized for the requested resource [6].

VIII. Existing Security Mechanisms

This section has a brief overview of the security mechanisms adopted by the cloud computing service providers to ensure customers security and privacy.

Table II. provides a brief of some existing cloud services and the methods adopted to handle issues which are listed in column 2 of the table.

TABLE II. Existing trends of handling issues.

Service	***Issue***	***Addressed by***
Amazon S3	Data Confidentiality Issue	ACL
Google Apps	Risk of Unauthorized use Data availability Issue	Distributed file systems, different sign-in options
Amazon EC2	Data Confidentiality Issue	Configuring OS.

Service	***Issue***	***Addressed by***
Amazon Virtual Private Cloud (VPC)	Data confidentiality Internet Accessible Management APIs can be compromised	Isolation of resources and encryption.
Windows Azure	Confidentiality	Adoption of SSL based APIs

A. Amazon S3

Access control lists (ACLs) at the bucket/object level are used to grant user access, which is authenticated via the user's signature with his/her private key . The security options include single sign-on, administrator-based single sign-out, policy-enforced secure mail transfer, secure browser connections, etc.

B. Google Apps

Uses a distributed file system designed to store large amounts of data across large numbers of computers. Structured data is then stored in a large distributed database built on top of the file system. Data is chunked and replicated over multiple systems such that no one system is a single point of failure.

C. Amazon EC2

Guest OS runs in a lesser-privileged mode, and applications are in the least privileged mode. Host OS can only be accessed by administrators of AWS. Customers have full access to their guest OS and can configure multi-factor authentication

D. Amazon Virtual Private Cloud (VPC)

Enables to use isolated resources that one owns within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec virtual private network (VPN) connections via identity and access management, isolation, and encryption.

E. Windows Azure

The identity and access management mechanism adopts service management API (SMAPI) to provide web services via the Representational State Transfer (REST) protocol, which runs over SSL and is authenticated with a certificate and private key generated by the customer.

IX. Conclusion

Cloud computing is always being improved so that clients can access various levels of on-demand services. Although there are many advantages to cloud computing, one major issue is security. Clouds still have a lot of vulnerabilities and hackers are still finding ways to use them. Security holes must be found in order to offer cloud users a higher standard of service. Numerous studies are being conducted to address concerns such as network security, data protection, virtualization, and resource separation. Gaining the user's trust in cloud applications and services is necessary to solve these problems. A significant issue in cloud computing is building user confidence, which can be done via building trust for cloud resources and apps. Trust management is becoming increasingly popular. There is a higher potential in the cloud environment, which can be exposed when the security challenges as stated in the paper are worked upon.

References

[1] David. "Cloud Security Risk, Threats, and Challenges" CrowdStrike. June 17, 2021. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threatschallenges/

[2] Issa M.Khalil , Abdallah Khreishah ,Muhammad Azeem "Cloud Computing Security : A Survey",March 2014 ,doi: 10.3390/computers3010001

[3] Bernd Grobauer, Tobias Walloschek, Elmar Stocker "Understanding Cloud Computing Vulnerabilities" ,June 2010, doi: 10.1109/MSP.2010.115

[4] Danish Jamil,Hassan Zaki "Security Issues in Cloud Computing and Countermeasures",International Journal of Engineering Science and Technology, April 2011.

[5] Mukesh Kant Tripathi I , Vivek Kumar Sehga "Establishing Trust in Cloud Computing Security with the Help of Inter-Clouds" ,2014 IEEE International Conference on Advanced Communications,Control and Computing Technologies

[6] Mohammad Ubaidullah Bokhari , Qahtan Makki Shallal , Yahya KordTamandani "Security and Privacy Issues in Cloud Computing",Jan 2016, Transaction of the International Conference on Endodontics,International Conference on Endodontics

[7] Marwan Darwish,Abdelkader Ouda,Luis Fernando Capretz "

Cloud-based DDOS attacks and defenses", January 2013 , IEEE International Conference on Information Society (i-Society 2013), pp. 67-71, 2013

[8] Ashish Singh,Kakali Chatterjee "Cloud Security Issues and Challenges:A Survey, November 2016 ,Journal of Network and Computer Applications , doi :10.106/j.jnca:2016.11.027

[9] Avijit Mondal and Subrata Paul,Radha Tamal Goswami,Syam Nath "Cloud Computing security issues and challenges : A Review", 2020 International Conference on Computer Communication and Informatics(ICCCI)

[10] Buyya R,Murshed M. GridSim:A toolkit for modeling and simulation of distributed resources management and scheduling for grid computing,2022 ,Concurrency and Computation:Practice and Experience/Volume 14,Issue 13-15/p.1175-1220

[11] Manish Mahajan and akashdeep Sharma "Steganography inColoured Images Using Infor mation Reflector with 2k Correction" 2010 International Journal of Computer Application(0975-8887).

[12] Randeep Kaur,Jagroop Kaur "Cloud Computing Security Issues and its Solution: A Review" ,Dec 2014 , 2015 2^{nd} International Conference on Computing for Sustainable Global Development

[13] Neha Kajal,Nikhat Ikram,Prachi "Security Threats In Cloud Computing", July 2015 ,doi:10.1109/CCAA.2015.7148463

[14] Dimitrios Zissis,Dimitrios Lekkas "Addressing Cloud Computing Security Issues"., March 2012 ,Future Generation Computer Systems 28(3):583-592 , doi:10.1016/j.future.2010.12.006

[15] Amara Naseer,Huang Zhiqui,Awais Ali "Cloud Computing Security Attacks with Their Mitigation Techniques", October 2017,International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,doi:10.1109/CyberC.2017.37

[16] Russell Brandom "The CPU catastrophe will hit hardest in the cloud", Jan 2018,The Verge

[17] Suryateja S. Pericherla ,"Cloud Computing Threats,Vulnerabilities and Countermeasures: A State-of-the-Art", Jan 2023 ,Security in Cloud Computing and IoT ,doi:10.22042/isecure.2022.312328.718

[18] Sabah M.Alturfi,Bahaa Al-Musawi and Hayder Abdulameer Marhoon ,"An advanced classification of cloud computing security techniques:A survey" AIP Conference Proceedings 2290,040017(202),doi:10.1063/5.0027355

[19] Deng-Guo Feng,Min Zhang,Yan Zhang,Zhan Xu "Study on Cloud Computing Security",Journal of Software ,Volume 22 (1) (2011) ,Issue 1,pp 71-83

[20] Akintoye Kayode A. "Security and Reliability Issues in the Deployement of Cloud Computing System", July 2015 ,Oman Chapter of Arabian Journal of Business and Mangement Review 2(7):84-90 ,doi:10.12816/0019105.