Webology (ISSN: 1735-188X)
Volume 18, Number 3, 2021

A Study On The Security Requirements, Risk Identification, And Threats Associated With Cloud Computing

Minhaj khan[1] , Mohammadi Akheela Khanum[2]

[1]Integral University,Lucknow

[2]Integral University, Lucknow

ABSTRACT

Cloud figuring may be termed Internet-based computing, in which communal assets, software programs, and facts are made handy on request. The cloud computing setup offers smooth-to-get right of entry to the carrier for personal and private bases &records. Cloud computing has received significant recognition due to uninterruptedly growing desires over the last long time. Organizations that migrate to cloud-based annals storage solutions reap a slew of benefits. It reduces the rate and complexity of carrier corporations thru the fashion of belongings and active charges. The global is watching a tremendous growth inside the cloud-aided services and is foreseen to expand in addition with the stepped forward technological revolutions. It lets in patrons to get proper entry to drivers tenuously. Despite the enormous rewards of the Cloud computing paradigm, cloud figuring has mounted to have a few barriers and downsides, primarily regarding privateness of consumer's facts and protection associated danger. Since this technology's assemblies rely upon the Internet, a character cannot get the right of entry to their applications, server, or data from the mist, so outmoded safety shape does not follow here due to the truth the client does no lengthier very own the infrastructure anymore. This paper consists of the dangers and protection issues allied with Cloud Figuring. The storyline assessment provided in this paper gives cloud care issues and requirements, recognized risks, and threats. This artwork goals to investigate the appealing gears of cloud computing similarly to offer protection and privateness problems that this placing faces and observe in-depth know-how about the safety danger factors that cloud entities calm with cloud worker companies face on a regular foundation.

Keywords: Cloud Computing, Service models, deployment models, Cloud computing security requirement

I. INTRODUCTION

Cloud including is more than a CPU issuer or a manner of handing over calculating services; it is revolutionizing the adding landscape and developing huge technological and fiscal adjustments. Cloud computing gives customers a community-based sincerely settings imaginative and prescient, letting them percent calculations and resources no matter wherein they may be physically positioned. Productions that adapt to cloud-primarily based statistics storing get a bunch of blessings. It reduces deal providers' fees and complexity with the valuable resource of reducing asset and operational expenses. Cloud-primarily based fully offerings are getting increasingly famous spherical the place, and this trend is probable to keep as technology grows. It permits clients to peer encoding on a sporadic basis. It is a dynamic carter that uses the Internet to run customers with obfuscated digital sources [13]. This approach can bid entree to a massive form of on-call for services. Cloud computing is based on virtualization thought. A huge unmarried gadget (i.e., server) is shared with the aid of using several customers for whom everyone has their very own set of capitals [1, 5].

Cloud computing is defined by the National Institute of Standards and Technology (NIST) [26] as "an idea for allowing a pervasive, convenient, on-demand pool of configurable computing resources pool of programmable calculating sources." The developments include self-employment on demand, access to a considerable civic, property pooling, rapid elasticity, and measured carrier. [25]. It indicates the Hybrid, Community, Private, and public cloud placement kinds. The 3 issuer fashions, PAAS (Platform as a Deal), IAAS (Setup as a Service), and SAAS (Deal as a Deal), are then joint (Software as a Package).

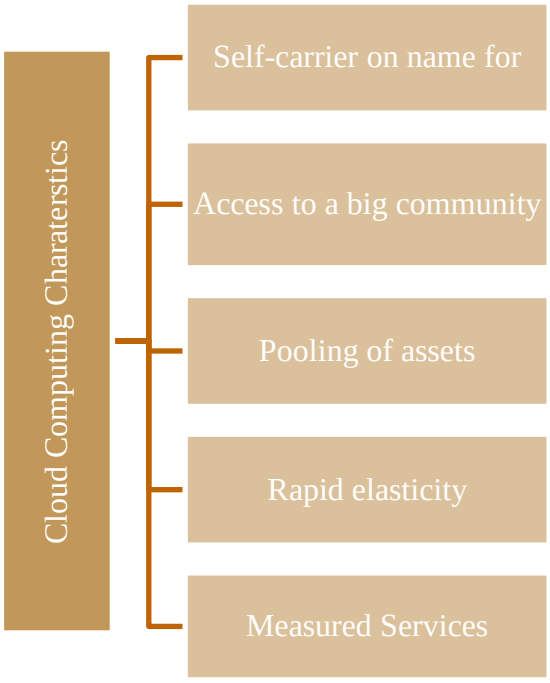

Fig1: Characteristics of Cloud Computing

Self-carrier on the name for: It permits clients to get the right of getting admission to paintings and accumulate offerings minus postpone using on items and jogging interfaces, without the want for human involvement [16].

Access to a big community: Data and hubs inside the cloud need to be had from a ramification of devices, which incorporates cellular headphones, computing device computers, and CPU computers. These devices use enterprise-popular strategies and era to function. As for the character of cloud computing, it wants that permits you to merchandise all the identical dated protocols [16].

Pooling of assets: The cloud company makes large sizes of actual or virtual computing property available to various customers in a multi-tenant engine. Those properties are dynamically allocated [16].

Rapid elasticity: The cloud provides an essential function. By scaling out, a client can brief collect more excellent properties from the cloud, after which decrease in discharging the ones causes even as they will be no lengthier desired. Customers have to get proper access to an endless variety of assets, which they should buy as wanted on a pay-consistent with-use foundation [16].

Measured Services: Each occupant's beneficial supply usage is chased, monitored, delimited, and optional. This presents each earner and the client with responsibility. The cloud engine includes a metering eye that can be used for song billing, applicable reserve use, and first-rate pay for what turned into used [16].

II. CLOUD COMPUTING SERVICE MODELS AND DEPLOYMENT MODELS

There are four deployment types, as depicted in figure 1&figure 2, and per the National Institute of Standards and Technology (NIST) [19].

Software as Service (SaaS)	Platform as Service (SaaS)	Platform as Service (SaaS)
• Clienteles can use drivers which is probably hosted on a cloud server and served through the Internet the custom of SaaS, frequently referred to as on-call for company. Application software application, going for walks structures, and numerous capitals are controlled and managed via cloud service vendors. Since the underlying shape in addition to the implementation platform is out of the person's attain, SaaS has the least range of shelter manipulate [26].	•The nature of a pc platform through the net is idea PaaS. PaaS refers to a cloud hauler commercial enterprise who gives, runs, and maintains each tool software and in addition figuring assets. Users are neither required to buy their private scheme or software application, nor are they crucial to pay for professional transfer of those assets. PaaS offerings encompass all gears of app development, together with format, development, and web hosting.The PaaS paradigm bounces greater suppleness and protection control to customers than SaaS, however a lot much less than IaaS.[26]	•Construction as a Service (IaaS) is the cloud-based totally definitely virtualization of computing assets full of tool, workstations, recollections, working structures, connectivity, and media. It licenses customers to get right of entry to all property even as now not taking to shop for any physical tool. IaaS is likewise a value-powerful and quicker way to run workloads deprived of having to buy or prevail the causal enterprise company; even though, as it is predicated on Internet get skip to, disposal is a key hassle. [26]

Figure 2: Cloud Computing Service Models

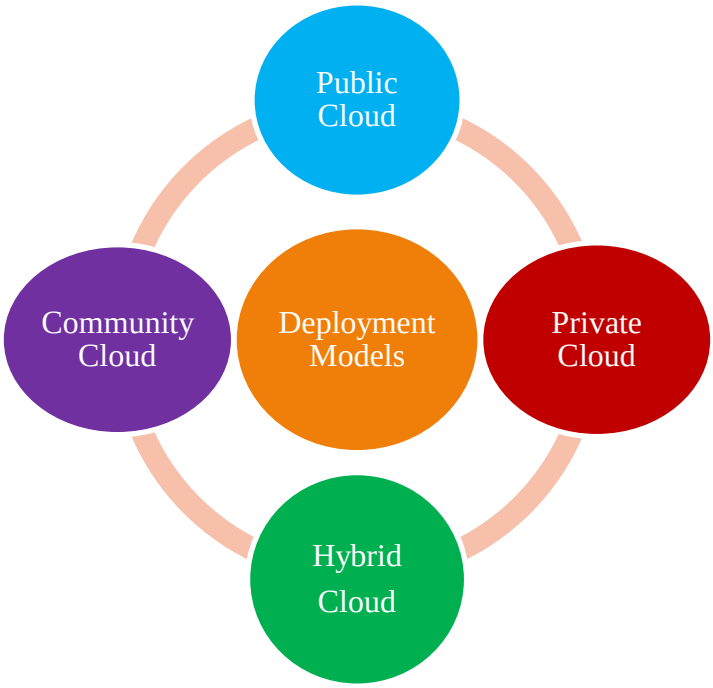

Fig 3:The Certain Models of Cloud Deployment

Public Cloud: Hardware and software property are not unusual overtly among commonplace users or most essential corporation businesses in public cloud environs. This surrounds is managed and monitored with the valuable resource of a third-celebration public-cloud earner employer, which tops up in several demanding situations which are inconvenient for customers. Clients have no idea what kind of garage the CSP uses, where their facts are housed physically, or where the unit stores their records (i.e., specific multi-tenancy problems). As an end outcome, even when transferring to the public cloud, businesses should compromise on key defense elements [19, 28].

Private Cloud: Cloud offerings are solely for a single company, and the cloud can be on-premises or off-premises, and it can be skillful with the reserve of the enterprise or a 3rd-celebration. A personal cloud is exorbitant because motion is accountable for all infrastructure manipulation and renovation. While Private Cloud overpowers Civic Cloud's safety troubles, it moreover provides overheads such as storage abilities, recital monitoring, and provisioning [19, 28].

Hybrid cloud: A hybrid cloud trusts more effective vapors (non-public, network, or public). This deployment method is essentially based on the topographies of the clouds concerned, and it lets in for immoderate extensibility, similarly to an extensive exchange of records disposition options. A hybrid cloud can be administered from unmarried vicinity since the public cloud's privateness standards vary significantly from those within the far-off cloud. Data privacy and integrity worries rise when information moves from a public to a non-public cloud environment or vice versa [19, 28].

Community cloud: Public clouds are just like community clouds in masses of components; however, this cloud-carrier shape is typically tailored to exact human beings, organizations, or organizations with similar cloud requirements. Civic people or a third-birthday amassing company can run the joint bases in a civic cloud. The problem of this paradigm is that many lingering questions on provider disturbances, contractual and protection implications, and annals unfold in multiple firms and regions [19, 28].

Cloud adding, at the same time as additionally, its many dedications, has been set to have excessive limitations and downsides, pointedly in phrases of protection. Clienteles cannot get admission to their apps, servers, or statistics from the cloud because those structures depend on the Internet, so everyday protection structure no longer complies with the fact that the setup is not always saved through the patron. This paper delves into the dangers and security troubles that include cloud computing. The up-to-date assessment of this item discusses the problems and prerequisites for cloud safety in the calculation to acknowledge risks and threats. The main goal of this paper is to identify the different types of risks that come with cloud deployment models, then look at the various security requirements that cloud deployment models have, as well as

identify various types of threats, and finally find the most concerning risk among the security requirements that cloud company carters face daily.

III. THE RISK ASSOCIATED WITH THE DEPLOYMENT MODELS OF THE CLOUD

The danger of an occasion up to have a dreadful effect on the success of the dreams is known as a hazard. With cloud and non-Cloud organization assemblies, the nature of risks (i.E. Security, dependability, accessibility, and standard universal recital) is the same. However, contingent on the effect of dangerous occasions (residual and herbal) connected with the CSP, the Risk certificates and its profile range if Cloud solutions are carried out [13]. Liable at the client's desires and programs, a Cloud can be deployed in selecting strategies. Opening the danger degree and associated problems at each of these fashions becomes essential. To yet, no look at the need to focus on this problem considers. The deployment model is essential to trouble for each CSP and customers because the user must now rely upon the CSP's topology to fulfill his wishes, and vice versa, practical Risk, Organizational threat, criminal threat, and miscellaneous danger are times of cloud vicinity threat [13, 16, 24].

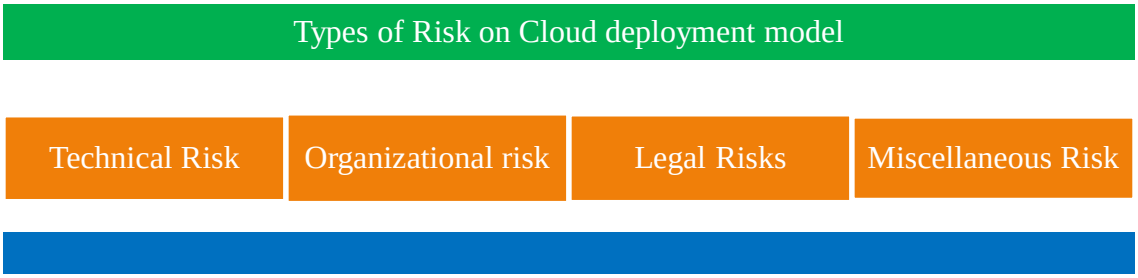

Fig 4:Risk classification in the cloud-based on the deployment model

Technical Risk: The simple olive way to tool and be a part of amongst consumer records structures and Cloud offerings is thru programming barriers (APIs) that the hauler issuer makes to be had to the person, generation-associated dangers exist. When there can be trouble with the API, it causes the hauler's complete or partial interruption. As a surrender effect, APIs threaten disposal and safety, in precise set the absence of manages. These technology-related plights affect deployment copies. Segregation failure, malicious insider, denial of the issuer, statistics copying, records nosy, lack encryption keys, cloud agency malicious insider, and so on are all risks allied with facts displayed.

Organizational Risk: Because of the quit of earner, there are risks to the business enterprise—deficiency in governance/failure in a salable enterprise, Power failure, Lock-in, Unauthorized issuer access.

Legal Risk: Administrations regularly function in plenty of jurisdictions with several regulatory requirements, which leads to slight non-compliance problems. As personal statistics privateness

regulations vary from nation to kingdom [23], the institutions of the empire wherein its cloud is deployed can also have to get real access to rights to the possessions housed in this one. Client property is in danger of statistics privacy because of a lack of expertise of sovereignty. Selected prison dangers are Regulatory non-compliance, the risk from changes of jurisdiction, Licensing dangers, Data shield risks.

Miscellaneous Risk: Network control, Snarls out of place, stolen/ Backup associated problems, Usual disaster, Illicit get right of front to premises/ Unauthorized get proper of access to the device, Theft of computer package/ Theft of PCs.

IV. NOTATIONS & CLOUD COMPUTING SECURITY REQUIREMENTS PARAMETERS

There are eight different security requirements or parameters for cloud computing: confidentiality, integrity, availability, authentication**,** authorization, accountability, privacy, non-repudiation. [19, 26, 28].This review will use the notations R1, R2, R3, R4, R5, R6, R7, and R8 to indicate security requirements. In table 1, the meanings of various notations are explained.

TABLE I: NOTATIONS AND THEIR MEANING

Notations	Security Requirements Parameters
R1	Confidentiality
R2	Integrity
R3	Availability
R4	Authentication
R5	Authorization
R6	Privacy
R8	Non-repudiation

R1: It ensures that information is not always uncovered or made available to unauthorized human beings, organizations, or traces if it has far stowed non-public [19,26, 28].

R2: It ensures that information acquired by authorized personnel is entirely identical to the data submitted. Put another way. It makes data more accurate and complete in the face of data manipulation faults, unanticipated phenomena, or unauthorized applications [19, 28].

R3: It guarantees that services are obtainable to authorized users and that information is obtainable and usable at the same time as desired. For example, an allotted denial-of-service (DDoS) bout disables a gadget's capability to inventory statistics. In the case of information, it refers to the assurance of annals access internal time or timetable hints [19, 26, 28].

R4: It refers back to the self of the cloud person, the starting place of the consumer's data, and content cloth fabric authentication. It is, in fact, the approach of setting up sincerity as a basis for being given as accurate with. Data integrity and privacy, in truth, are lone excessive best if the senders' and recipients' identities are effectively mounted [26, 28].

R5: It Grants the authenticated cloud user access to the subscription cloud services at the appropriate level [26, 28].
R6: Itrefers to the principles of openly assigning responsibilities for information system resource supervision and holding assignees accountable to proper authorities for the stewardship of resources under their control. The person in charge of information security keeps track of what is going on [26].

R7: Privacy is the ideally suited crucial kingdom in the discipline of cloud computing since all clients' facts are saved on cloud servers and examined via cloud facilities. Personal records include the entirety from non-public pix to monetary gen to instant documents [26].

R8: It concerns the ability to show the occurrence of a claimed action and the parties involved. The purpose of non-repudiation is to ensure that the authorized person cannot deny the validity of their activities [28].

V. THREATS ON CLOUD SECURITY REQUIREMENTS

Apart from the advantages that cloud computing offers, there exist many safety threats that prevent clients from hypnotic those advantages. Those protect threats are defined, agreed upon, and are commonly conventional in this segment. Table.2 highlights care threats in cloud computing and cloud offerings they have to an effect on.

Data breaches: For cloud consumers, the risk of a data breach is a significant concern. In reality, a records breach takes area even as sensitive or personal annals, which incorporates credit score card numbers or Social Security numbers, is leaked, accessed, obtained, and life castoff for malicious reasons.[26]

Hacked interface and application software program interfaces: Claim software program layout interfaces (APIs) are provided to cloud shoppers for monitoring, provisioning, orchestration, and transfer of their assigned sources, exposing the cloud figuring surroundings to the outside universal and potentially to attackers. Web facilities are often used to construct and implement one's APIs. Still, they have flaws. These APIs too can be used to provide charge-

brought services, perhaps giving a third party get right of front to the individual's credentials. [26]

Account hijacking: Cloud model hijacking is at the equal time as an assailant steals or takes control of a cloud account. Cloud account takeover is a common identification robbery technique wherein an attacker uses stolen account statistics to perform destructive or unauthorized travels. In reality, even as a cloud account is hacked, the aggressor regularly uses stolen credentials to ape the account proprietor. Attackers might use stolen IDs to gain entrée to sensitive areas of cloud computing systems, endangering their safety, truth, and obtainability. [29]

Malicious insider: A malicious insider is a modern or former worker, or any employer associate, who has or has crook get proper of ahead-facing to an information tool and has, will certainly misuse that get admission to compromise the info gadget's guard and privateness. A malicious insider is someone who gets get right of entrée to a business enterprise's Internet, tool, or information and releases it without the enterprise's consent. Insiders may be upward thrust up as vicious for a diffusion of reasons, together with retribution, coercion, ideology, ego, or financial assist via critical belongings robbery or espionage [10,26, 29].

Distributed denial of Service: A Renunciation of Deal attack is one of the most common resources of threat within the cloud. The assailant often sends many puzzling requests to a single provider. When the Cloud Computing effective device detects an immoderate strain at the flooding provider, it boosts the available dispensation size to deal with more weight. On the only hand, the cloud carrier employer fights the attacker; then over, the cloud company aids the attacker with the valuable resource of letting it abuse its assets, version the created facility unavailable to real clients [10, 22]

Abuse and Nefarious Use of Mist Services Unaccounted for, mismanaged, faux, loose trails discrete debts then inadequately secured cloud placements is probably accountable, allowing attackers to get right of getting entry to laptop stuff and abuse them to purpose victims. Disseminated email, unwelcome mail, denial-of-company assaults, and phishing attempts are only a few examples of how cloud-based completely absolutely presents are misused. [26]

Shared Technology: The sharing of generation, every for setup, systems, and applications is at the coronary heart of the cloud calculating system. The workings that facilitate technology sharing in multi-tenant environs, in which many clients' applications are hosted together, are often no lengthier designed to provide a fundamental isolation characteristic. This can also want to disclose common era to weaknesses, which contain virtualization troubles. [10, 26]

Ambiguous possession &responsibility: Lack of flat ownership and defined duties for information safety may also result in failing to fulfill controlling and statistics crook responsibilities. [17]

Malware Attacks/Difficult Impostor Detection: Cause kits, Trojan horses, Cross-Site-Scripting (XSS) attacks, and taints are samples of such attacks. Because numerous people from many amazing customers utilize the cloud, it is far tough to be aware of intruders. [17]

Data Loss: Accidental loss, inadvertent damage, or physical calamities consisting of fireplace, earthquake, flood, or distinctive herbal disappointments can all result in the eternal lack of saved outsourced facts till it is miles sponsored as a lot as a secure website available to the prison client.[10,26]

Insufficient Due Diligence: Lone cloud-exceptional abilities and functionalities are advertised, but there are no data approximately inner protection protocols, configurations, patching, logging, or auditing. About problems (who has to get a rate to, does the vendor offer records, in which may be statistics held, and so forth) are frequently left out, sendoff clients with an unsure chance profile that might pose easy dangers. [17]

Regulatory & Legal Issues: Since personal figures, protection suggestions range employing the usage of using state., the authorities within the united conditions of us in which the cloud is positioned also can have to get admission to the property stored there. Due to a lack of sovereignty information, customer assets are susceptible to information discretion and privateness. [16, 17]

Data Scavenging: An assailant may be able to get higher dynamic information because records cannot be wiped if the device is destroyed. [17]

Service Disruption: A engine breakdown, the unattainability of cloud offerings, or the cloud business enterprise's inadequate beneficial supply capacity motive saleable corporation operations to be disrupted [17]

Data Leakage: After documents get into the rude palms, however being moved, stored, edited, or assessed. [17]

Data lock-in: Clienteles cannot retrieve gen or programmed from one platform to every exclusive due to a lack of constancy in storage software program programming interfaces. [17]

Data Inconsistency: Discrepancies in connections with internal systems reason statistics inconsistency risks. The reason is colorful safety, which incorporates numerous customers' insertion, deletion, and trade. Administrative mistakes, fraudulent computation services. [17]

Identity Theft: When someone else's certification is used to get proper access to data or an application, privacy and fact are jeopardized. [17]

Business Continuity: There is a casualty that a cloud hauler company will exit of business enterprise for technical or non-technical troubles. [17]

Phishing Attack: A move at social engineering Version or carter hacking occurs because of spammers engineering stabbings on haze providers. [17]

Weak identification, Credential, and Access Management: As a final consequence, attackers' affectation as criminal clients get unlawful get right of information entry, resulting in gen breaches that may be hazardous to the information proprietor and distinct stakeholders. [26]

System and Application Vulnerabilities: This puny point is due to weaknesses in tool and alertness software program, which enemies have to type the intense to scouse borrow statistics and take control of the edifices. All services and annals are accidental while contacts in a waged tool's libraries, kernel, and claim tools exist. Multi-tenancy, which desires the center of musing and belongings in many schemes from specific agencies housed inside the same cloud settings, runs, however higher dose base. [26]

Natural disasters, which include disasters, can probably damage the correct and redundant copies of data in a files canter. As a cease result, availability is once more jeopardized, and appropriate steps to record those states need to be taken. [22]

IP spoofing: It is a famous road costing approach. In truth, the attacker sends a message to a relied-on laptop man or woman, after which the ruse obtains the man or woman's IP address, alters the packet's header, and sends a bundle deal that airs as if the ruse person's primary package deal. [10, 29]

Information disclosure: Information can be leaked to unintentional recipients because of unethical movement. Information can be stolen from the tool in a change of strategies, including collecting digital tool configurations and looking for open ports to find aids and vulnerabilities. The kinds of disclosures that might arise in a cloud device are necessary and extrinsic disclosures. When a worker or administrator mistakenly makes private information civic, that is known as an internal disclosure. It would possibly arise due to a loss of obliteration, negligence, mistakes, or a failure to know the significance of fabric. An outside annals disclosure attack seeks gadget-precise statistics approximately a business enterprise, consisting of cloud website hosting, individuality numbers, and patch levels. The backup or transitory documents area is probably protected with the accrued records. [29]

TABLE II: THE IMPACT OF CLOUD COMPUTING THREATS ON CLOUD SECURITY PARAMETERS

S.No.	Threats	R1	R2	R3	R4	R5	R6	R7	R8
1	Abuse of Cloud Services	✓		✓					✓

2	Insecure interfaces &APIs	✓	✓	✓		✓	✓	✓	
3	Shared Technology	✓	✓	✓			✓	✓	
4	Malicious Insiders	✓	✓	✓	✓			✓	
5	Ambiguous ownership						✓		
6	Account or Service hijacking	✓	✓	✓	✓	✓	✓	✓	✓
7	Malware Attacks	✓	✓	✓			✓		
8	Data Loss			✓			✓		✓
9	Insufficient Due Diligence	✓	✓	✓	✓	✓	✓	✓	
10	Denial of Service			✓					
11	Data Breaches/ Data Theft	✓						✓	
12	Regulatory & Legal issues	✓					✓		
13	IP spoofing				✓				
14	Service Disruption			✓					
15	Data Leakage	✓					✓		
16	Data lock-in			✓					✓
17	Data Inconsistency		✓						
18	Identity Theft	✓	✓						
19	Business Continuity			✓			✓		
20	Phishing Attack	✓							
21	Weak identity	✓	✓	✓	✓	✓	✓	✓	

22	System and application vulnerability	✓	✓	✓	✓	✓	✓	✓	
23	Natural Disaster			✓					
24	Information disclosure	✓							

Requirement legends: R1: Confidentiality, R2: Integrity, R3: Availability, R4: Authentication, R5: Authorization, R6: Accountability, R7: Privacy, R8: Non-repudiation.;✓: Impact of threats on security parameters.

The following table 3summarizes the discussion in the preceding table 2.

TABLE III: THE THREATS AND THEIR DESCRIPTIONS BASED ON TABLE II

S.No.	Threats	Description
1	Abuse of Cloud Services	It impacts confidentiality, availability, and non-repudiation. Misuse of cloud resources comprises Assaults, phishing attempts, email spam, and digital crypt ocurrency "mining."
2	Insecure interfaces &APIs	Intruder, transparent verification, content transmission; restricted monitoring and logging capabilities; API dependencies influence confidentiality, integrity, availability, authorization, accountability, and privacy.
3	Shared Technology	Confidentiality, integrity, availability, accountability, and privacy are all affected. It has weaknesses, ineffective access restrictions, and influence over the runtime environment. There is a chance you will allow access to other consumers' sensitive information.
4	Malicious Insiders	Because of intelligence gathering, hacking, organized crime, corporate espionage; spoofing, malicious attacks, disclosure requirements, country sponsored intrusion, Brand malfunction; implications; lost production, impact on business continuity, &traditional security, Confidentiality, Integrity, availability, authentication, and privacy are all endangered.
5	Ambiguous ownership	It affects accountability. Inability to satisfy regulatory and contractual information responsibilities may occur due to a lack of transparent management and defined responsibilities

		for data protection.
6	Account or Service hijacking	Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability, Privacy, and Non-repudiation are all affected. Account or service hijacking involves an attacker gaining access to identities and passwords, tracking activity and events, distorting records, falsifying details, and diverting to unauthorized websites.
7	Malware Attacks	It is difficult to identify an intruder in a malware assault since the cloud is accessible by various users from various clients using the device. As a result, Confidentiality, Integrity, Availability, and Accountability are all affected.
8	Data Loss	Data loss has a catastrophic business impact; it damages a company's brand and reputation; it affects stakeholders' morale and trust; it causes collateral damage and leads to infringements and legal repercussions. It has an impact on non-repudiation and accountability.
9	Insufficient Due Diligence	Software upgrades, code modifications, susceptibility profiles, penetration attempts, and security measures all determine a company's security conduct. Insufficient due diligence impacts Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability, Privacy, and Non-repudiation.
10	Denial of Service	It impacts availability because when this threat attacks the system, it causes system slowdowns, disruption of services, traffic bottlenecks, angry customers, and bill rises for consumers since the attacker consumes disc space, compute cycles, or CPU utilization, among other things.
11	Data Breaches/ Data Theft	While necessary to avert disastrous data loss, offline storage systems raise the risk of data breaches. As a result, it has an impact on data confidentiality and privacy.
12	Regulatory & Legal issues	Consumers' applications and services are kept on cloud providers that are undisclosed or untrustworthy, posing a danger of data and applicable privacy and confidentiality being compromised. As a result, it has an impact on Confidentiality and Accountability.
13	IP spoofing	Reflective Distributed Denial of Service (DDoS) assaults are frequently caused by spoofing Internet traffic, which is a

		constant danger. IP spoofing is used to get around the authentication of IP addresses. As a result, it has an impact on authentication.
14	Service Disruption	It affects availability. The cause is a breakdown in company operations, the absence of cloud services, or the cloud provider's inadequate resource availability.
15	Data Leakage	When data turns out wrong during data transfer, storage, manipulation, or monitoring, it challenges confidentiality and accountability.
16	Data lock-in	Information leakage, rising prices, and providers' business disruption impact availability and non-repudiation.
17	Data Inconsistency	due to inconsistencies in internal process interfaces, it is also caused by dynamic updating - many consumers' insertion, elimination, and alteration; administrative faults, dishonest computation services, which impact integrity.
18	Identity Theft	Confidentiality and integrity are jeopardized when someone else's credentials are used to obtain information or an application.
19	Business Continuity	There is a chance that a cloud service provider needs to go out of business for technical or non-technical problems, resulting in data loss and unfavorable publicity. As a result, it affects availability and accountability.
20	Phishing Attack	Account or service hacking occurs due to phishing attempts against cloud providers. As a result, it has a significant effect on confidentiality.
21	Weak identity	Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability, and Privacy are all impacted by a weak identity.
22	System and application vulnerability	It impacts Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability & Privacy.
23	Natural Disaster	Flash floods, fires, earthquakes, and other natural calamities are extremely difficult to predict or prevent. It affects

		availability.
24	Information disclosure	Data confidentiality prevents inadvertent, illegitimate, or unauthorized access, disclosure, or illegal access. The disclosure of information has a direct impact on confidentiality.

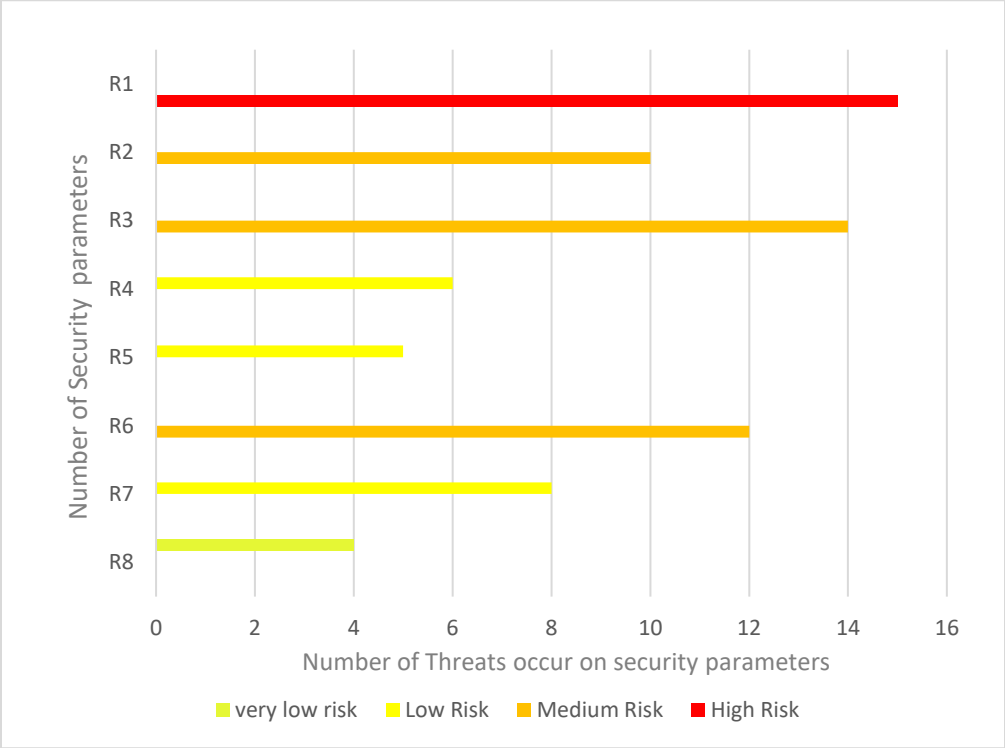

Fig 5: A large number of threats occur on security requirements parameters.

VI. CONCLUSION

Cloud services have become a vital part of organization lifestyles, offering a significant opportunity to decorate up a corporation corporate business enterprise's increase via their competence to unexpectedly enlarge, allowing us to be beneficial resource flexible, and permitting us to cooperate in new methods. Cloud computing, in truth, has a slew of rewards for businesses, businesses, or even nations. Despite the advantages, because the cloud has allocated making, the protection threat has quickly become a hotbed in Cloud computing studies. It takes air at seems on the orderly shape of dangers inside the cloud computing deployment paradigm. The leading aim of this examination is to expose all the capacity security risks in cloud computing placing The paper references the most pressing protection issues and the safety necessities for contemporary Fog homes. The reason for this paper is to provide a more exhaustive evaluation of that faintness as a manner to emphasize the significance of identifying

and addressing safety flaws in Cloud computing fashion. Lastly, several troubles associated with cloud safety requirements have appeared. Based on our findings and research in tables 2 and 3, we discovered that confidentiality is the most concerning risk in cloud computing security requirements. As a result, we will use this security requirement in future studies to mitigate the cloud security risk.

Acknowledgement: Manuscript Communication Number (MCN): IU/R&D/2021 – MCN0001332 office of research and development, Integral University, Lucknow.

REFERENCES

1. Xuan Zhang, Nattapong Wuwong, HaoLi, Xuejie Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments," 2010 10th IEEE International Conference on Computer and Information Technology, IEEE,2010
2. Mariana Carroll, Alta van der Merwe, "Secure Cloud Computing: Benefits, Risks, and Controls," IEEE,2011
3. Farzad Sabahi, "Cloud Computing Security Threats and Responses," IEEE,2011
4. Gurudatt Kulkarni & Jayant Gambhir, Tejswini Patil, Amruta Dongare, "A Security Aspects in Cloud Computing," IEEE,2012
5. Nathalie Brender 1, Iliya Markov, "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies," International Journal of Information Management, Elsevier,2013
6. Rohitash Kumar Banyal, Pragya Jain, "Multi-factor Authentication Framework for Cloud Computing," 2013 International Conference on Computational Intelligence, Modelling and Simulation, IEEE,2013
7. Daniel W.K. TSE, "Challenges on Privacy and Reliability in Cloud Computing Security," IEEE,2014
8. R. Velumadhava Raoa,*, K. Selvamanib, "Data Security Challenges and Its Solutions in Cloud Computing," International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015), Elsevier,2015
9. Arab Dutta, Guo Chao Alex Peng & Alok Choudhary, "Risks in Enterprise Cloud Computing: The Perspective of it Experts," Journal of Computer Information Systems, 10 December 2015
10. S.Mahdi Shariati, Abouzarjomehri, M.Hossein Ahmadzadegan," Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection," KBEI, IEEE, 2015
11. Syed Asad Hussain, Mehwish Fatima, AtifSaeed, ImranRaza, Raja Khurram Shahzad, "Multilevel classification of security concerns in cloud computing," Applied Computing and Informatics, Elsevier, April 2016

12. Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills, "Data Security in Cloud Computing," Fifth International Conference on Future Generation Communication Technologies (FGCT 2016), IEEE,2016
13. Prachi Deshpande, S. C. Sharma, Sateesh K. Peddoju, Ajith Abraham, "Security and service assurance issues in Cloud environment," Springer,2016
14. Nabeel Khan, Adil Al-Yasirib," Identifying Cloud Security Threats to Strengthen Cloud Computing
15. Adoption Framework", The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies(IoTNAT' 2016), Elsevier,2016
16. Chaimaa Belbergui, Najib Elkamoun, Rachid Hilal,"Cloud Computing: Overview and Risk Identification Based on Classification by Type",IEEE ,2017
17. Ahmad, H. Bakht, U. Mohan, "Cloud Computing – Threats and Challenges," JOURNAL OF COMPUTING AND MANAGEMENT STUDIES VOLUME 1. ISSUE 1. 30TH JANUARY 2017
18. Talal Halabi, Martine Bellaiche," Towards quantification and evaluation of the security of Cloud Service Providers," Journal of Information Security and Applications, Elsevier, January 2017
19. Pradeep Kumar Sharma, Prem Shankar Kaushik, Prerna Agarwal, "Issues And Challenges of Data Security In A Cloud Computing Environment," IEEE,2017
20. Teófilo Branco, Filipe de Sá-Soares, Alfonso Lopez Riverob, "Key Issues for the Successful Adoption of Cloud Computing," Science Direct, Elsevier,2017
21. Steve Jones, "Risks and rewards of cloud computing in the UK public sector, A reflection on three Organisational case studies," Springer, 12 April 2017
22. Srijita Basu, Arjun Bardhan, Koyal Gupta, PayelSaha, "Cloud Computing Security Challenges & Solutions-A Survey," IEEE 2018
23. Harikrishna Pillutla, Amuthan Arjunan, "Fuzzy self-organizing maps-based DDoS mitigation mechanism for software-defined networking in cloud computing," Journal of Ambient Intelligence and Humanized Computing, Springer, 15 March 2018
24. Frederik Wulf, Susanne Strahringer, Markus Westner, "Information Security Risks, Benefits, and Mitigation Measures in Cloud Sourcing," IEEE 21st Conference on Business Informatics (CBI),2019
25. Dr. Aarushi Kataria, Dr. Naveen Nandal and Dr. Ritika Malik, Shahnaz Husain -A Successful Indian Woman Entrepreneur, International Journal of Disaster Recovery and Business ContinuityVol.11, No. 2, (2020), pp. 88–93
26. Kumar, S. (2020). Relevance of Buddhist Philosophy in Modern Management Theory. Psychology and Education, Vol. 58, no.2, pp. 2104–2111.
27. Roy, V., Shukla, P. K., Gupta, A. K., Goel, V., Shukla, P. K., & Shukla, S. (2021). Taxonomy on EEG Artifacts Removal Methods, Issues, and Healthcare Applications. Journal of Organizational and End User Computing (JOEUC), 33(1), 19-46. http://doi.org/10.4018/JOEUC.2021010102

28. Shukla Prashant Kumar, Sandhu Jasminder Kaur, Ahirwar Anamika, Ghai Deepika, Maheshwary Priti, Shukla Piyush Kumar (2021). Multi objective Genetic Algorithm and Convolutional Neural Network Based COVID-19 Identification in Chest X-Ray Images, Mathematical Problems in Engineering, vol. 2021, Article ID 7804540, 9 pages. https://doi.org/10.1155/2021/7804540
29. Gurmeher Singh Puri, Ravi Tiwary, Shipra Shukla, "A REVIEW ON CLOUD COMPUTING," IEEE, 2019
30. Rakesh Kumar, Rinkaj Goyal, "On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey," computer science review, Elsevier,2019
31. Abdul Raoof Wani, Q.P. Rana, U. Saxena, Nitin Pandey, "Analysis and Detection of D DoS Attacks on Cloud computing environment using Machine Learning Techniques," IEEE,2019
32. Hamed Tabrizchi, "A survey on security challenges in cloud computing issues, threats, and solutions," The Journal of Supercomputing, Springer, 28 February 2020
33. Riddhi Doshi, PG Scholar, Vivek Kute, "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), IEEE,2020
34. Vijaya Kumar Veerabathiran, Devi Mani, Sangeetha Kuppusamy, "Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption," Springer, 06 July 2020