IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Adoption of the Cloud Control Matrix Framework for Effective Measurement at Cloud Risk, Threat, Attack, and Vulnerability

[1]Umma Khatuna Jannat, [2]Dr.M.MohanKumar, [3]Syed Arif Islam

[1]Research Scholar, [2]Associate Professor, [3]Research Scholar
[1]Computer Science,
[1]Karpagam Academy of Higher Education, Coimbatore, India.

Abstract: Cloud computing is a convoluted framework that empowers wanted administrations by joining an assortment of arranged gadgets. Cloud computing is comprised of a few kinds of configurable dispersed frameworks with different degrees of network for use. Associations are quickly taking on cloud networks because of benefits like expense viability, versatility, unwavering quality, and adaptability. The possibility clients expect to take on the cloud, however, its security issues impact clients' trust in its administration. As of now, there are numerous information security frameworks, standards, and guides to defend associations from security threats, but these are not specific to cloud organizations. The Cloud Security Alliance (CSA) has delivered Cloud Controls Matrix Version 4 (CCM v4.0), distributed in the last year of 2021 to give security controls, especially to cloud organizations. The Cloud control matrix (CCM) and it provide the various controls that need to be implemented by the service provider to avoid/reduce/mitigate the risks related to the service provided. This research paper provides an overview of the implementation of the cloud security alliance model. We have identified a total of 26 cloud security risks, threats, attacks, and vulnerabilities. We mapped it into a CCM to test its effectiveness measurement and find out if the CCM identified solution is the best security control or not.

***Index Terms* - risk, threat, attack, vulnerabilities, cloud, matrix, measurement.**

I. INTRODUCTION

Cloud computing uses a combination of hardware and software to deliver various processing, storage, and analysis capabilities via a network. Thanks to cloud computing, users can easily access files and use services such as Gmail, Dropbox, and Skype from any device via the internet. The cloud is a large pool of virtualized resources that are both accessible and useable. As a result of low prices, cloud computing platforms have become the most significant and well-known thing in the IT industry. Major corporations such as Microsoft, Amazon, and Google have adopted cloud computing. The cloud computing system is made up of two parts: the front end and the back end. The front end is the user end, or user interface, through which the user accesses cloud services via devices. The back end of the system is a cloud where all of the services and data are stored [1] [2]. The cloud structure is well-known for its services, which have attracted a lot of interest from businesses. Cloud computing is also encountering numerous barriers in its implementation, which, if not addressed promptly, could pose a significant challenge to its rapid growth [3]. Users are concerned about security, especially when sending secret or sensitive data to a cloud server [4]. In truth, most cloud servers are controlled by industrial agencies that are not within the user's control. Furthermore, when building a risk profile while phasing into a cloud storage paradigm, it's critical to identify information assets. The deployment and distribution models that are employed are determined by security and privacy issues.

1.1 Deployment Models

1.1.1 Public Cloud

The public cloud has a marginally alarming name, yet it doesn't mean shared information. It implies a third-party supplier, most notably Amazon Web Services. Google Cloud Platform provides cloud administrations on-demand, either over the public web or to committed organizations. Generally, it's finished with a solitary occupancy, which implies a solitary case like a server, accessible per client, which brings greater security consolation. Nonetheless, because it saves money on monetary and natural effects, multi-occupant public distributed computing is progressively utilised for arranging, testing, and advancement. It's likewise famous for its enormous AI and quantum registering jobs. The public cloud is well known and widely used by organisations worldwide in light of the fact that the main cloud suppliers can ensure uptime across the globe. As compensation, the public cloud reacts well to capricious client use and adaptability. Many consider pooling assets in the public cloud to be a less expensive choice than others. The danger of the public cloud, and particularly of utilising this discounted overabundance figure, is that it could run out [5].

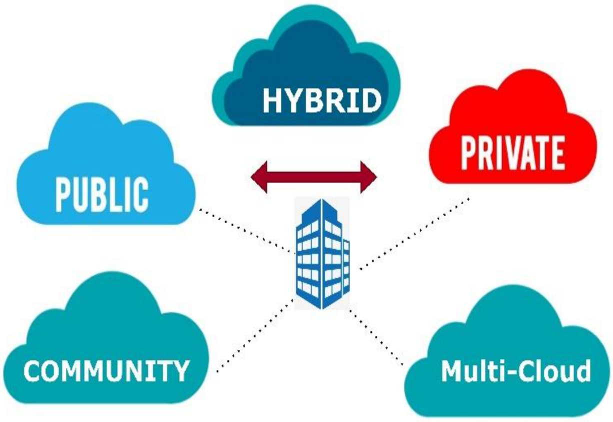

Fig. 1. Deployment Models

1.1.2 Private Cloud

The private cloud deployment model differs from the public cloud deployment methodology. For a single person, it's a one-on-one situation (customer). Sharing hardware with others is not required. It is a term that depicts an individual's capacity to utilise frameworks and administrations inside a specific association or limit. The cloud stage is introduced and overseen by an association's IT office in a safe cloud-based environment protected by strong firewalls. It's run solely for the advantage of a single corporation. It can be managed in-house or by a third party, and it can take place on-site or off-site.

1.1.3 Community Cloud

It enables a group of organisations to gain access to frameworks and administrations [6]. It's a circulated framework that unites the administrations of numerous clouds to fulfil the needs of a local area, industry, or business. Associations with comparable worries or errands could share the local area's foundation. An outsider or an alliance of at least one local area association is ordinarily accountable for staying up with the latest.

1.1.4 Hybrid Cloud

A hybrid cloud is a cloud computing system that combines an on-premises private cloud with public cloud services through orchestration. This typically necessitates the creation of a connection between an on-premises data centre and a public cloud. Other private assets, such as edge devices or other clouds, could be included in the link. In a hybrid cloud model, businesses run workloads on internal IT infrastructures or public clouds, then switch back and forth as computing demands and costs change. This gives a business greater data deployment options and flexibility. A hybrid cloud workload includes all of an application's network, hosting, and web service functionalities. While the terms "hybrid" and "multi-cloud" are frequently used interchangeably, they have major differences. A hybrid cloud is a unified environment that blends on-premises, private resources with public cloud resources supplied by AWS, Microsoft, and Google. A multi-cloud infrastructure is made up of two or more public cloud providers, with no private or on-premises components. An effective hybrid cloud approach requires a solid network connection. For added security, a wide area network or dedicated networking service is usually used. A corporation should assess its connection regularly to ensure that it fulfils the uptime standards outlined in the service-level agreement with a cloud provider.

1.1.5 Multi-cloud

The term "multi-cloud" refers to the use of at least two distributed computing administrations from a variety of cloud vendors. A multi-cloud framework can be completely closed, completely open, or a hybrid of the two. Multi-cloud frameworks are used by businesses to improve asset registration and reduce the risk of blackouts and data loss. The handling and capacity limits of an enterprise can likewise be helped through association. Cloud progression has brought about a move from single-client private clouds to multi-occupant public clouds and hybrid clouds.

1.2 Architecture Models

The way these innovation elements come together to form a cloud, where assets are pooled and shared across an enterprise, is referred to as cloud architecture. A front-end stage (the consumer or gadget used to access the cloud), a back-end stage (servers and capacity), a cloud-based delivery mechanism, and a network are all components of a cloud design. These technologies work together to form a cloud computing infrastructure on which applications may run and end-users may access cloud resources. Organizations can use cloud computing to decrease or eliminate dependency on an on-premises server, storage, and networking infrastructure. A cloud architecture enables businesses to move IT resources to the public cloud, replacing on-premises servers and storage, as well as IT data centre real estate, cooling, and power, with a monthly IT cost. One of the main reasons for cloud computing's current popularity is the shift from capital investment to operating expense.

1.2.1 Infrastructure as a Service

Infrastructure as a service (IaaS) is a type of cloud computing in which virtualized computing resources are delivered via the internet. IaaS is one of the three basic categories of cloud computing services, along with software as a service (SaaS) and platform as a service (PaaS). In the IaaS model, the cloud provider manages IT infrastructures such as storage, server, and networking resources and makes them available to subscribers via virtual machines that can be accessed over the internet. Organizations may use IaaS to make workloads faster, easier, more flexible, and cost-effective.

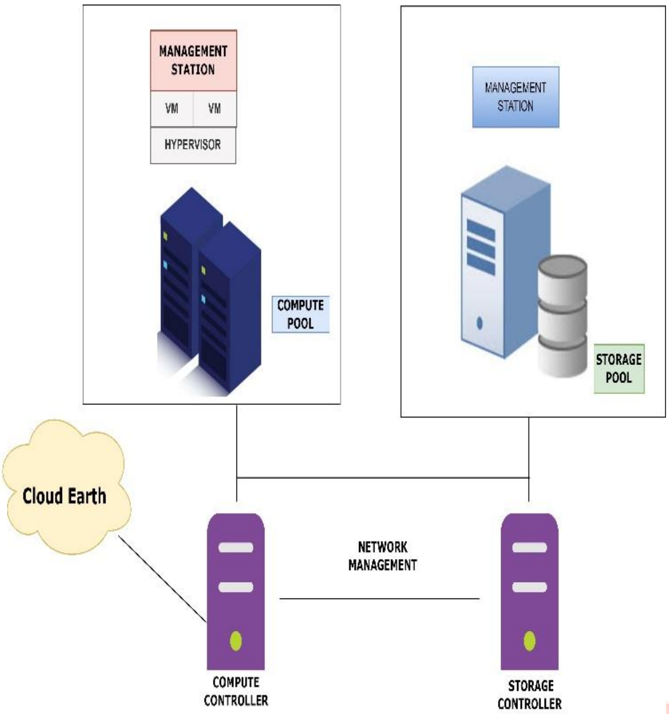

Fig. 2. Infrastructure as a Service

Organizations pick IaaS because running a workload without having to buy, manage, and support the underlying infrastructure is frequently easier, faster, and more cost-effective. A company can easily rent or lease infrastructure from another company using IaaS. Under the IaaS service paradigm, a cloud provider hosts the infrastructure components that would otherwise be located in an on-premises data centre. This includes the hypervisor (virtualization) layer, as well as servers, storage, and networking equipment. In addition to the infrastructure components, IaaS companies offer a variety of services. Just a few examples include detailed billing, monitoring, log access, security, load balancing, and storage resiliency, such as backup, replication, and recovery. This service is becoming more policy-driven, allowing IaaS users to more fully automate and orchestrate critical infrastructure operations [5] [6]. For example, to ensure application availability and performance, a user can design policies to drive load balancing. IaaS users connect to resources and services across a wide area network, such as the internet, and then complete the application stack using the cloud provider's services. For example, the user can log into the IaaS platform to build Virtual Machines (VMs), install operating systems in each VM, deploy middleware such as databases, create storage buckets for workloads and backups, and install the enterprise workload onto that VM. Customers can then track costs, monitor performance, balance network traffic, solve application difficulties, and manage disaster recovery using the provider's services. Any cloud computing model necessitates the involvement of a provider. A third-party entity that specialises in selling IaaS is frequently the provider. Independent IaaS providers include amazon web services and google cloud platform. A company might even set up its own private cloud and become its own infrastructure provider.

1.2.2 Platform as a Service

Of all the models, PaaS is the hardest to authoritatively portray due to both the wide scope of PaaS contributions and the numerous methods of PaaS administration. PaaS adds an extra layer of incorporation with application improvement structures, middleware capacities, and capacities like data sets, informing, and lining. With PaaS, the cloud client oversees applications and middleware while the cloud supplier handles the virtualization, information, organizing, runtime, administration, and capacity.

PaaS offers a total web improvement climate and is normally equipment freethinker. Maybe, in particular, PaaS abstracts and robotizes out a portion of the huge intricacy that accompanies Kubernetes. Along these lines, it likewise reduces the expense of keeping up with all of the above, including the need to enrol exceptionally particular DevOps modellers. The organization gets a feeling of control while the cloud supplier is liable for security, robotization, and autoscaling. PaaS eliminates these managerial concerns, allowing groups to focus solely on conveying business value [5] [6].

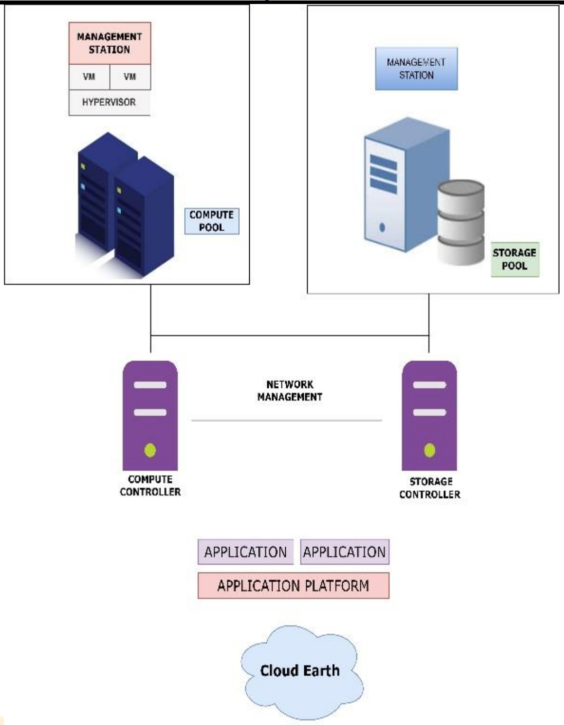

Fig. 3. Platform as a Service

1.2.3 Software as a Service

SaaS administrations are multitenant, full-featured applications with all of the structural intricacies that accompany any large programming stage. SaaS is frequently alluded to in the same way as business programming. Salesforce is the old norm in this gathering. However, Zoom, Dropbox, Office 365, and the Google App Suite are similarly ubiquitous among new companies through ventures. It's a completely supervised experience in the cloud, sitting at the highest point of the programming stack. Simply use the apparatuses; they will run every part of them. Given the increased dexterity, power, and financial advantages of IaaS and PaaS, numerous SaaS organisations have grown on top of them [7].

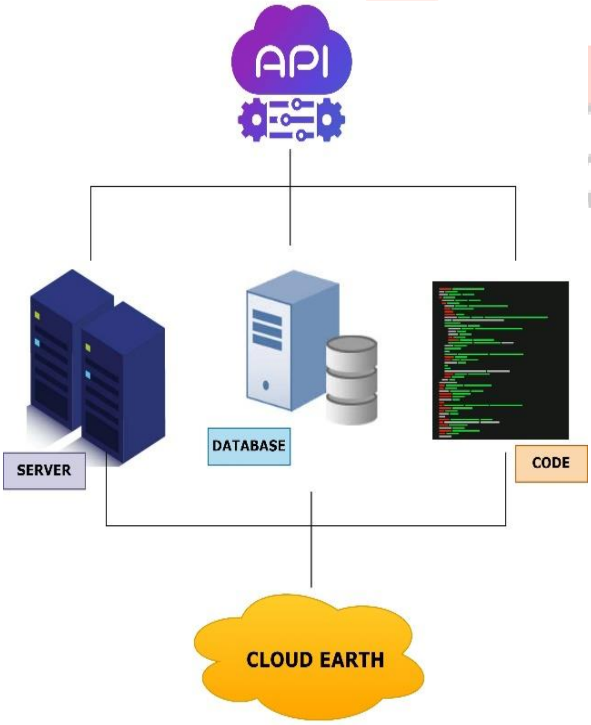

Fig. 4. Software as a Service

1.2.4 Function as a Service or Serverless Compute

FaaS represents Function as a Service, or Serverless Compute. Function-as-a-Service (FaaS) is a type of distributed computing administration that allows code execution based on events without the perplexing foundation normally associated with the development and deployment of microservices applications. It assists in eliminating the intricacies of servers and gives a serverless design. With FaaS, the actual equipment, virtual machine working framework, and web server programming board are taken care of by the cloud specialist organization.

1.3 Security Issues Affecting Cloud Security

When it comes to choosing cloud providers, cloud security is a big worry for customers. Consumer trust in cloud services should be based on adequate security information, but in fact, security information is critical and may not be made public. However, the majority of cloud service providers do not provide accurate information about their security. Information security controls should be chosen and executed in proportion to the risks, which is normally done by assessing threats, vulnerabilities, impacts, and probability of occurrence. In various surveys on cloud computing adoption, information security, loss of control, and other problems are regularly identified as the top main reasons for enterprises hesitation to employ cloud services. Enterprises want guarantees that using the cloud will not put their organisation in danger. Ironically, virtualization and multi-tenancy, which enable much of the cloud's scalability, elasticity, and potential cost savings, are at the root of many of these security and privacy issues. Traditional IT security perimeters are challenged by the dynamic nature of big virtualized infrastructures that may span multiple geographic locations and involve assets beyond the direct control of the organisation [5-10].

Even if data is managed by a third party, the consumer retains responsibility for securing data to the end customer, internal or external, as the data owner. Encryption is one of the answers, but encrypting data in storage, data in transit, and key management has practical and business restrictions. The data that is currently in use is still susceptible. Another key difficulty that cloud consumers face is the ownership of cloud services. A cloud customer signs an agreement with a cloud service provider, who then signs an agreement with a service provider, such as Amazon Cloud, to provide the service. In reality, the provider may rely on other service providers (storage, network, application, processing, and so on) who are not obligated to the cloud customer. These reliances may vary without the consumer's knowledge, especially when cloud service providers are striving to meet elasticity and price goals. At any given time, the consumer has no idea where their data is or how it is being properly protected. This trust could expose the consumer to dangers that aren't covered by the contract and for which the consumer has no direct legal recourse.

II. IDENTIFYING CLOUD RISK, THREAT, ATTACK, AND VULNERABILITY

One of the primary issues with cloud computing is security. As a result, researchers are more concerned about cloud security. In this part, we look at the most common security dangers and concerns associated with cloud computing. These are the primary guidance hazards that enterprises should be aware of before implementing any cloud interface or services.

Despite its enormous promise, cloud computing has yet to be adopted by consumers with the passion and speed that it merits. The gaps can be blamed for this. A threat is something that will occur, and it is one of the factors that determine the appearance of risk [8] [9] [10]. Dangers to cloud services are identified here, as well as threats in the context of the cloud that can interrupt cloud services. Vulnerabilities in cloud computing, as well as those that are concerning [11] [12]. There might be plenty of ways of describing, which is intensified by the way that many gatherings are associated with the expansion of cloud suppliers and customers. Analysts led a fast but exhaustive examination of distributed computing security, distinguishing the fundamental advantages, disadvantages, and cost-security tradeoffs [13].

We recently surveyed the security chances presented by the crucial idea of various help conveyance structures [14]. An overview of cloud stages was embraced, with an emphasis on the establishment, stockpiling framework, foundation administration, and reconciliation [15]. Researchers sought to identify cloud architectures based on the classifications, which included survey findings on existing cloud services [16] [17]. This paper explains the advantages of a secure cloud as well as various security risks and existing mitigation measures. Although there are some good security research projects, they are limited in scope and incomplete. As a result, decided to write an article on cloud security dimensions. Here are the top identified cloud risks, threats, attacks, and vulnerabilities in Table I. All these are identified in details

1. Backdoors

   A backdoor attack is a type of breach in which hackers employ deceit and proper concealment to install malware that can circumvent a network's regular security and authentication requirements. Once a backdoor has been discovered, it is difficult to determine properly patched all of the holes. Spyware is a sort of spyware that, once installed on a machine, collects information on a person, including the websites visit on the internet, the items download, the files open, usernames, passwords, and anything else of value. In a backdoor attack, hackers first look for a weak point or a compromised programme on the device to exploit [18]. This could be a vulnerability in an application, an unsecured port on the network, or a weak password on an account.

2. Formjacking

   While formjacking is not a new threat, the number of cases has recently increased dramatically. For example, Symantec's software discovered and prevented over 3.7 million formjacking attempts. Hackers insert malicious javascript code into a website, usually an e-commerce site where a user is expected to provide personal information that is intercepted and copied [19]. They can be thought of as an online version of skimmers, which are used by crooks to steal credit card information from ATMs, or someone peeping over a customer's shoulder and writing down whatever enter. The strategy is divided into three stages. An attacker first acquires access to a website's core code and then puts the malicious script onto a specific web page, which is typically part of the site's checkout area. Then, when an unwary user goes to that page to make a purchase, the customer submits personal information, including a credit card number. Finally, when clicking "submit," an extra copy of the data is made, which is transmitted directly to the hacker, in addition to being sent to the merchant's website for processing. Hackers then have everything needed to perpetrate fraud or identity theft, including a person's name, address, phone number, and most importantly, full credit card information.

TABLE I. LIST OF CLOUD RISK, THREAT, ATTACK, VULNERABILITY IDENTIFICATION

Serials	List of Cloud Risk, Threat, Attack, Vulnerability Identification
1.	Backdoors
2.	Formjacking
3.	Cloud Cryptojacking
4.	DNS Poisoning Attacks
5.	Drive-by Downloads
6.	Exploits and Exploit Kits
7.	External Data Sharing
8.	Log4Shell
9.	Social Engineering
10.	Cloud Provider Malicious Insiders
11.	SQL Injection Attack
12.	Man in the Cloud Attack
13.	Operational Technology (OT)
14.	Zero-Day Attacks
15.	Pixel Flood Attack
16.	Server-Side Request Forgery (SSRF)
17.	Cyberattacks
18.	Insider Attacks
19.	SaaS Layer Attacks
20.	PaaS Layer Attacks
21.	IaaS Layer Attacks
22.	Cloud AI Powered Attacks
23.	VM Escape Attacks
24.	Cloud Phishing Scams
25.	Crypto Cloud Mining
26.	Absence of Cloud Security Architecture and Strategy

3. Cloud Cryptojacking

Cryptojacking is defined as the "unauthorised use of victim computing resources to mine and exfiltrate coins" [20]. It's a sort of malware, or malicious software, that's designed to infect or damage computers, servers, and networks. To mine cryptocurrencies successfully and profitably, dedicated hardware such as graphics processing units and application specific integration circuits is required. Those who cannot afford to buy the hardware turn to illicit methods of accessing computational resources to mine bitcoin for themselves, such as the ones listed below:

- Malicious browser extensions
- Cryptojacking in the browser
- ISP and public router hacking through cryptojacking via android apps
- Third-party libraries that have been hacked

4. DNS Poisoning Attacks

Because of a security vulnerability in the DNS infrastructure, providers may be vulnerable to server attacks. DNS spoofing attacks that aren't very complex focus on deceiving or diverting a user to a strange website [21]. Individuals with keen eyes and a high level of security awareness will immediately recognise these spoofing attempts for what they are and avoid them. However, attackers can use this DNS vulnerability to send victims to deliberately fake addresses that look identical to their real counterparts. "gmail.com" or "bankofamerica.com" will be seen by potential targets.

5. Drive-by Downloads

In a typical attack scenario, the threat actor compromises the victim's machine and recruits it into a botnet. Control of the user's device can be abused by the attacker [22]. This occurs in the following manner:

- Injection: The attacker embeds or injects a malicious element into a hacked web page. This can take the form of javaScript code, a link, a redirect, a malvertisement ad that executes malicious code when viewed or clicked, or cross-site scripting (XSS).
- Vulnerability Exploits: When a user enters a page, the dangerous element is activated. A weakness in a segment of the user's computer's software stack is exploited by the element. This could be due to vulnerabilities in the browser, browser plugins, the operating system, an archiving tool such as WinZIP, a file reader such as Adobe PDF, older multimedia delivery systems such as Adobe Flash or Microsoft Silverlight, or Java version flaws.
- Download: This component sends harmful files to the user's device invisibly. In this situation, the payload is a Trojan horse. Attackers may also use other payloads.
- Execution: The Trojan horse executes, revealing a shell that the attacker can use to take control of the device.

6. Exploits and Exploit Kits

An exploit is an attack on a computer system that makes use of a specific vulnerability that the system exposes to intruders [23]. The action of successfully initiating such an attack is referred to as an exploit. Exploits can be launched in several ways, but one of the most common is through rogue websites. The victim may accidentally visit such a site or be misled into clicking on a link to the malicious site in a phishing email or a malicious advertisement. Exploit kits, which are software toolkits that comprise malicious software that may be used to launch attacks against many browser vulnerabilities from a malicious or hacked website, may be installed on malicious or hacked websites used for computer exploits. These attacks usually target java-based software, unpatched browsers, or browser plug-ins, and are often used to infect the victim's computer with malware.

7. External Data Sharing

Data sharing is made simple on the cloud. Many clouds allow to send an email invitation to a collaborator or provide a link that allows anyone with the URL to view the shared resource. While the ease with which data may be shared is a benefit, it can also be a major cloud security concern. It's tough to limit access to a shared resource when utilising link-based sharing, which is a popular option because it's easier than directly inviting each intended collaborator. The shared link can be forwarded, stolen as part of a cyberattack, or guessed by a cybercriminal, allowing unauthorised access to the shared resource. Furthermore, link-based sharing makes it impossible to restrict access to just one recipient of the shared link [24].

8. Log4Shell

By delivering a malicious text string to hacked web-facing servers, threat actors can utilise the Log4shell attack to seize control. It's part of Log4shell, an open-source Apache module for recording the faults and events of java-based applications. The chatbox is used to enter this harmful string. Text placed into the username box on web apps, such as Apple iCloud, can also initiate the intrusion. Log4shell is a widely used Apache library, with millions of java programmes and applications. As a result, determining the exact number of internet-facing applications affected by the Log4shell flaw is nearly impossible. The vulnerability is expected to affect devices and services from major giants such as Apple, Amazon, Tesla, and Twitter, according to researchers. This vulnerability, which is being aggressively exploited by an expanding collection of threat actors, offers an important challenge to network defenders given its widespread. Easterly's agency has labelled Log4shell "important," a comment repeated by similar organisations around the world, including Germany's national cybersecurity agency. Log4shell received a 9.8 CVSS score from enterprise software vendor Redhat, while the NIST gave it a 10—the best attainable [25].

9. Social Engineering

Social engineering attacks account for a large percentage of all cyber attacks, and studies show that they are becoming more prevalent. Phishing is a common type of social engineering attack that begins more than 90% of successful hacks and data breaches. Cunning social engineers use deceit to induce victims to provide private or sensitive information [26]. A social engineer can use this information to expand attacks once a victim has been deceived into providing it. Phishing is a social engineering technique in which an attacker sends emails that appear to be from a reliable source. In general, phishing casts a wide net and tries to reach out to as many people as possible.

10. Cloud Provider Malicious Insiders

While businesses spend a lot of money to protect data from unauthorised access from the outside, dishonest workers steal the data. According to the 2021 Data Breach Investigation Report, internal actors were responsible for 36% of all data breaches recorded by big organisations in 2020. For small and medium businesses, it was 44% [27]. Malicious insider attacks can have a wide range of serious consequences for businesses, ranging from the loss of secret data, revenue, and clients to reputational damage and even the closure of a company. According to the US Computer Emergency Readiness Team (CERT), a malicious insider is a current or former employee, contractor, or trusted business partner who exploits access to important assets in a way that affects the organisation. Malicious insiders are more difficult to spot than outside attackers since they have legitimate access to an organization's data and spend the majority of their time executing ordinary work activities.

11. SQL Injection Attack

SQL injection, often known as an insertion, is a malicious attack that specifically targets SQL-based applications. Hackers can use SQL to insert arbitrary code into SQL queries, allowing them to directly add, modify, and delete records from a database. SQL attacks can compromise any website or web application that makes use of a SQL database, such as MySQL, SQL Server, Oracle, and others. To initiate a SQL attack, an attacker finds a weak input into a website or web application [28]. To exploit this vulnerability, use user input in the form of a SQL query. The attacker employs a specially prepared SQL command as a cyber intrusion. The code aids in obtaining a response that provides a clear view of the database's structure, allowing full database access. The types of SQL attacks differ depending on the database engine.

12. Man in the Cloud Attack

In recent years, the amount of data and information that has been moved to the cloud and stored on various cloud-based platforms has skyrocketed. Cloud-based services like Microsoft OneDrive, Google Drive, and Dropbox have been found to improve these operations. Anyone can set up a low-cost or even free synchronisation service between local folders and cloud-based counterparts with a few mouse clicks. The advantages of using cloud-based services include file sharing, automated data backup, system-independent cloud data access, and collaboration from anywhere and at any time. Due to malicious entities with the intent of stealing data, such services turn into disadvantages, making the entire scenario of using cloud services a highly risky one, given the sensitivity of data under transmission in the cloud.

"Man in the cloud" attack is a new strategy devised by some of these sophisticated cybercriminals. The ability of cloud storage to "access data from anywhere at any time" is used in these attacks. The application that syncs with the cloud service uses a synchronisation token to gain access to the appropriate account and data. To install malware on the targeted systems, also known as switchers, the attackers primarily use social-engineering operations in combination with malicious attachments in emails [29]. The potential victim's synchronisation token is moved to the data-sync folder when malware is executed. The attacker's token would then be swapped out for the original one. When targeted programmes sync with data-sync envelopes again, the target's unique token is copied to the attacker's cloud sites, where it can be easily accessible and used in the future by those attackers. This gives attackers access to the victims cloud-based data from any computer machine, allowing them to sync harmful files in place of those that the user ordinarily trusts. It's done in such a way that most of the evidence of the attacks is lost.

13. Operational Technology (OT)

Critical vulnerabilities in popular cloud management software have emerged in the push to shift operational technology (OT) and industrial control systems to the cloud [30]. The flaws can be exploited remotely, allowing an attacker to get access to a cloud management console with a single hacked field device or to take control of many programmable logic controllers and OT devices through a single compromised workstation. The flaws could potentially allow an attacker to physically harm equipment and gadgets connected to a hacked network.

14. Zero-Day Attacks

An attacker will combine zero-day vulnerabilities into a vulnerability charting list and with processing programme payloads intermingled, resulting in the influence of an attack on the server [31]. More often than not, zero-day attackers spend hours, months, or weeks manipulating attacks across lines of code to find the system's weakness. Following the discovery of a system flaw, the attacker concentrated on the target apps. Attackers always trace networks to find flaws to get access to the network and execute. In this way, the network is infiltrated and a zero-day attack is launched. There is no adequate process in place when a zero-day attack is discovered within the network. A typical zero-day attack prevention approach is used in the detection of vulnerabilities and the production of the signature. Zero-day attackers have a high level of technical understanding and have been unknown to the public for a long time. As a result, detecting a zero-day attack is considered a difficult undertaking.

15. Pixel Flood Attack

This is a pretty simple technique that can be used to test any file upload facility that accepts photos. In a Pixel Flood Attack, an attacker attempts to upload a large-pixel-size file, which consumes server resources to the point that the application may crash. This could result in a simple application-level denial of service. To save storage and processing power, many current applications now use third-party libraries to process large photos and convert them to smaller images. However, several of these image processing libraries may be subject to the pixel flood attack, which can cause resource consumption or an application-level denial of service attack [32].

16. Server-Side Request Forgery (SSRF)

An attacker uses server functionality to access or modify resources in a SSRF attack. The attacker goes after an application that allows users to import data from URLs or read data from URLs. URLs can be changed by either replacing them with new ones or messing with the URL path traversal algorithm [33]. In most cases, attackers provide a URL (or modify an existing one), and the server's code reads or submits data to it. URLs can be used by attackers to obtain access to internal data and services that aren't supposed to be accessible, such as HTTP-enabled databases and server configuration data. The server gets the request after an attacker has tampered with it and attempts to read data from the altered URL. Even if a service isn't immediately accessible on the internet, attackers can choose a target URL that allows them to view the data.

17. Cyberattacks

Cybercrime is a business, and cybercriminals choose targets based on how profitable attacks are predicted to be. Cloud-based infrastructure is directly accessible from the public internet, is frequently insecure, and houses a lot of sensitive and important information. Furthermore, because the cloud is used by a wide range of businesses, a successful attack can be replicated many times with a high possibility of success. As a result, cyberattacks on cloud deployments are becoming more frequent [34].

18. Insider Attacks

Insider risks are becoming more prevalent in cloud computing. An insider threat is a security danger that originates within the target organisation. It frequently involves a current or former employee or business colleague who has unauthorised access to sensitive data or privileged accounts on the network of an organisation. Threatbusters: According to Bitglass 2019 insider threat report, 68 percent of 437 IT professionals questioned said firms were somewhat too severely exposed to insider attacks [35].

19. SaaS Layer Attacks

In SaaS layer attack, the majority of customers are concerned about data-related security issues such as data backup, data access, and data availability.

- DoS Attacks: DoS attacks, also known as denial of service attacks, are one of the most notable attacks in the cloud. The hacker's main goal was to exhaust all of the user's information by sending request packets across the internet.
- SQL Injection Attack: The ultimate goal of the SQL injection attack was to steal all user data from the internet, such as user names, passwords, credit card passwords, and so on, by injecting hostile cryptogram or other codes into the network as ordinary input. The hacker then gains unauthorised access to the user's data [36].
- Authentication Attack: Authentication attacks were possible due to the users' weak usernames and passwords. In this authentication attack, the hacker impersonates a user to trick the system and get unauthorised access.

20. PaaS Layer Attacks

The PaaS layer attack is also known as a side-channel or cross-site attack.

- Scanning Attack on the Port: This was a common exploit in which an attacker opened the portal address without authorization, extracted the information, and then destroyed or misused the information [36].
- Attack on Metadata Spoofing: In this case, the attacker gains access to the file and makes changes or deletes some critical activities.
- An Attack by a Man-in-the-browser: In this scenario, the attacker stands between the sender and the receiver and has access to the data.
- Phishing and spoofing attacks are four of the most common types of cyber-attacks. Both the server and the users will be affected by phishing or spoofing attacks. The user will be led to a fake web link, where the attacker will be able to access and obtain the user's personal information.

21. IaaS Layer Attacks

Attack on the IaaS layer Because there is a lack of protection opening in the virtualization administrator [36], the attack will occur frequently on this layer.

- Cross-virtual-machine Attacks: The side-channel attack is another name for this technique. Here, the user's sensitive information can be collected while some secondary data, such as power, volts, and minutes, is destroyed.
- Virtual Machine Rollback Attack: In this attack, the attacker obtains the virtual machine's password and uses it to take a snapshot and run it without the user's knowledge. A brute-force attack is used to carry out this attack. The assailant can also employ rollback, a permission management component, to change the user's accessibility or authorization code.
- Virtual Machine Escapes Attack: In this type of attack, the attackers attempt to disable guest operating systems or get access to memory data. After that, the attacker has complete control over the guest operating system.

22. Cloud AI Powered Attacks

Attackers will soon leverage AI and machine learning to boost the pace, scale, and sophistication of their campaigns. On numerous fronts, these highly focused and sophisticated threats are boosted, resulting in stealthier, faster, and more successful attacks [37]. No matter how frequently changed, AI attacks will always be one step ahead of static rules and signatures. Only defensive AI can effectively fight back against malevolent AI. Darktrace's Cyber AI engine detects innovative and sophisticated threats that elude signature-based techniques and delivers a surgical reaction at machine speed to stop cyber-attacks in infancy. To combat the emerging cyber-threat landscape, over 6,500 firms have added Cyber AI.

23. Virtual Machine (VM) Escape Attacks

The exploit method for virtual machine escape allows a guest-level VM to attack its host. The approach exploits a vulnerability in the VMware workstation when used in conjunction with cloud service provisioning software for cloud providers. An attacker uses code on a VM to allow an operating system running within it to break out and interact directly with the hypervisor [37]. A VM escape allows an attacker to gain access to the host operating system as well as all other VMs running on that host.

24. Cloud Phishing Scams

Phishing is a general term that refers to a type of social engineering attack that uses a variety of techniques to obtain user information, such as login credentials and credit card details. When an attacker tricks a victim into opening an email or text message, it is known as "phishing." When this malicious link is clicked, malware is installed and the machine is frozen, which can result in a ransomware attack or disclosure of important information [38].

A phishing attack can have disastrous consequences for both individuals and businesses. Businesses can suffer considerable financial losses as well as a loss of market share, reputation, and consumer trust, ranging from cash theft to broader attacks like APT. Anyone who uses the internet or phones might be a victim of phishing. Phishing attempts to infect a device with malware, steal money or identity, steal private credentials, and regain control of internet accounts.

25. Crypto Cloud Mining

The term "crypto mining" refers to the process of obtaining cryptocurrency by solving cryptographic challenges with high-powered computers. Validating data blocks and adding transaction records to the blockchain, a public ledger, are both parts of the process. Crypto mining, in layman's terms, is the process of collecting cryptocurrency as a reward for completing tasks. It is financially advantageous to target cloud structures for abuse. Cryptominers, in addition to ransomware, have spread rapidly. Cryptominers operate invisibly to be as permanent as possible, but ransomware is designed to be selective and self-destructive. Secretly, the victim's computer capacity is exploited to calculate cryptocurrency. According to the Verizon Data Breach Report 2020, 86 percent of data breaches were motivated by money, and the majority of them were perpetrated by external, coordinated attackers [27]. This pattern has now changed. In container-based cloud resources, attackers have discovered new prospective targets for crypto-mining attacks.

26. Absence of Cloud Security Architecture and Strategy

Attackers who employ cloud computing resources to target users, companies, and other cloud providers are abusing cloud services. Distributed Denial-of-Service attacks, phishing, email spam, and other forms of abusive use are only a few examples. Furthermore, because the malware in question leverages the CSP's domain, malevolent attackers can put malware on cloud services and make it appear more genuine. The malware that is housed in the cloud might also employ cloud-sharing tools as an attack vector to spread further. Companies should have more control over the entire cloud framework in 2021, while also keeping an eye on cloud services that are being targeted or abused by cybercriminals [39].

A cloud security architecture is a method for securing and viewing data and collaborative applications in the cloud for a business. This is done from the perspective of a cloud service provider. Organizations all across the world have been forced to move parts of IT infrastructure to public clouds as a result of the pandemic. To withstand cyberattacks, such a transformation necessitates the proper implementation of cloud security architecture. Data has been exposed to various risks due to a lack of an effective cloud security architecture and strategy. Organizations believe that by using a "lift-and-shift migration approach," in which the existing IT stack and security controls are moved to the cloud environment, apps and associated data may be migrated to the cloud. As a result, there is a misunderstanding of the shared security responsibility paradigm, which businesses must address to manage cloud security effectively.

III. CLOUD CONTROL MATRIX

The CSA Cloud Controls Matrix (CCM) is a cloud computing cybersecurity control system. The Cloud Security Alliance (CSA) published the Cloud Control Matrix Version 4 (CCM v4.0) in 2021 [18], which includes essential security and privacy controls as well as additional components. It's a spreadsheet with 17 domains that cover all of the major components of cloud computing.

There are 197 control objectives in each domain. It may be used to systematically evaluate cloud implementations by indicating which security controls should be applied by which actor in the cloud supply chain. CSA created the CCM as a set of information security policies to help businesses, particularly cloud-based businesses, identify the risks face [40]. The CCM Implementation Guidelines (which are contained in the publication), the Consensus Assessment Initiative Questionnaire (CAIQ), and the CCM Controls Auditing Guidelines are all examples of these. The CCM v4.0 additionally contains essential CCM control support information. It offers a complete set of security measures as well as a thorough understanding of security. There are 17 domains in Fig. 5 that are derived from well-known and widely accepted security standards, guidelines, recommendations, and legislation [14].

Given the nature of CCM controls, however, operationalization will be heavily influenced by the IT/service architecture, the type of technology utilised, the risks that must be managed, applicable regulations, organisational rules, and other significant considerations. It gives more inside and out security controls, especially corporate data security controls, to meet industry prerequisites for bringing down and distinguishing security risks, threats, attacks, and vulnerabilities in the cloud. As a result, the CSA is unable to provide precise, prescriptive counsel that applies to every company and cloud service deployment.

CCM 4 (CCM v4.0) is a free download that can assist enterprises in evaluating cloud providers and directing security initiatives. Cloud providers can also use the matrix to submit themselves to the CSA Security, Trust, and Assurance Registry (STAR), a free, publicly accessible registry that documents the security measures offered by cloud computing service providers. The CCM was created to work in tandem with the CAIQ, a series of yes-or-no questions for identifying specific themes that a customer would want to address with potential cloud service providers. The CSA CCM, as a framework, gives companies the structure, specifics, and clarity they need when it comes to information security requirements designed expressly for cloud computing.

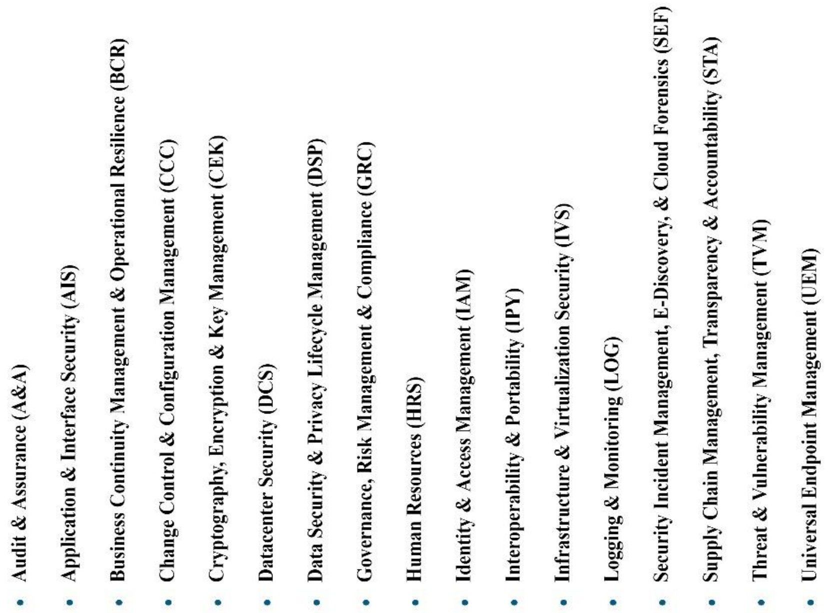
Audit & Assurance (A&A)
Application & Interface Security (AIS)
Business Continuity Management & Operational Resilience (BCR)
Change Control & Configuration Management (CCC)
Cryptography, Encryption & Key Management (CEK)
Datacenter Security (DCS)
Data Security & Privacy Lifecycle Management (DSP)
Governance, Risk Management & Compliance (GRC)
Human Resources (HRS)
Identity & Access Management (IAM)
Interoperability & Portability (IPY)
Infrastructure & Virtualization Security (IVS)
Logging & Monitoring (LOG)
Security Incident Management, E-Discovery, & Cloud Forensics (SEF)
Supply Chain Management, Transparency & Accountability (STA)
Threat & Vulnerability Management (TVM)
Universal Endpoint Management (UEM)

Fig. 5. Cloud Control Matrix 17 Domain Name

Methodology for Implementing a Cloud Control Matrix: In CCM v4.0, there are 197 controls structured. The amount of control in each domain varies. These controls are identified and assigned a unique number. Table II lists the domain name and the number of controls associated with it. The CCM specifies the requirements for each control associated with a certain domain area. These controls are also related to architectural relevance, which aids cloud consumers and providers in understanding the importance of things like physical servers, network computers, data storage, and applications. This assists organisations in determining the efficacy of using numerous standards and models.

There are 17 cloud security domains in CCM v4.0. These domains are mentioned in details below, along with a brief description. Due to paper size limitations, the details of each 197 control are not described here.

- Audit and Assurance
  6 control specifications make up the Audit and Assurance (A & A) domain. This domain is intended to assist the CSP and CSC in developing and implementing an audit management process that includes audit planning, risk analysis, security control evaluation, conclusion, remediation, report generation, and reviews of previous reports and supporting evidence.

- Application and Interface Security
  The Application and Interface Security (AIS) domain includes 7 control specifications to assist cloud enterprises in migrating to secure application and interface design, development, deployment, and operations in the cloud. The AIS controls aid enterprises in identifying and mitigating risks in cloud landscapes during the design and development phase of the application. In the deployment and operations phases, businesses must additionally assess cyber resistance to attacks by remediating vulnerabilities using complementing automation and manual code review.

TABLE II. DOMAIN NAME WITH CONTROLS

Domain Names	Controls
Audit & Assurance (A&A)	6
Application & Interface Security (AIS)	7
Business Continuity Management & Operational Resilience (BCR)	11
Change Control & Configuration Management (CCC)	9
Cryptography, Encryption & Key Management (CEK)	21
Datacenter Security (DCS)	15
Data Security & Privacy Lifecycle Management (DSP)	19
Governance, Risk Management & Compliance (GRC)	8
Human Resources (HRS)	13
Identity & Access Management (IAM)	16
Interoperability & Portability (IPY)	4
Infrastructure & Virtualization Security (IVS)	9
Logging & Monitoring (LOG)	13
Security Incident Management, E-Discovery, & Cloud Forensics (SEF)	8
Supply Chain Management, Transparency & Accountability (STA)	14
Threat & Vulnerability Management (TVM)	10
Universal Endpoint Management (UEM)	14

- Business Continuity Management and Operational Resilience
  CSPs and CSCs can use the Business Continuity and Operational Resilience (BCR) domain to ensure that the cloud services supply are reliable. The domain directs resiliency techniques, such as mitigation planning and implementation, to enable companies to continue operations in the face of anticipated and unanticipated disruptions. 11 control specifications make up the domain.

- Change Control and Configuration Management
  There are 9 controls in the Change Control and Configuration Management domain. These controls are intended to reduce the risks associated with changing the configuration of Information Technology (IT) assets by following a thorough change management procedure regardless of whether the IT assets are handled internally or externally. This domain ensures that IT asset configurations are only changed to an established baseline once the intended changes have been approved by the change management authority.

- Cryptography, Encryption and Key Management
  The Cryptography, Encryption, and Key Management (CEK) domain is made up of 21 control requirements that ensure data and keys are used to safeguard and secure data effectively. The CEK controls are divided into three categories: governance, risk management, and compliance. They are useful for governing policies and procedures, risk management, key lifecycle processing, and cryptographic key management systems, among other things.

- Datacenter Security
  This domain has 15 control standards that assist "Cloud Service Providers," or firms that provide data centre hosting services. These CSPs are expected to implement these specifications in order to protect the data held in the data centre for cloud service customers. Controls cover a wide range of data centre security topics. All of the controls in this domain are anticipated to be implemented, and all are equally important. This is also true for the rest of the domains.

- Data Security and Privacy Lifecycle Management
  In CCM v4.0, a new domain called "Data Security and Privacy Lifecycle Management" was added. It has 19 privacy and data security controls. These restrictions are not industry or sector specific, and are not targeted at a single country or law. On the other hand, these restrictions were created by taking into account the common aspects and requirements of significant privacy standards.

- Governance, Risk Management, and Compliance
  To support, define, and direct organisational security and compliance operations, the Governance, Risk Management, and Compliance (GRC) domain employs 8 control standards (specifically corporate and IT governance). By offering direction, tools, and solutions for establishing a secure environment and governance controls to aid in the management of confidentiality, integrity, and availability.

- Human Resources
  Human Resources (HRS) is critical to an organization's compliance structure's effectiveness. Personnel engagement with systems, technology, assets, and data is handled by human resources, which serves as a link between IT security and employees. There are 13 controllers in the domain.

- Identity and Access Management
  The Identity and Access Management (IAM) domain has 16 control specifications that address the mission-critical need to assure appropriate resource access in increasingly heterogeneous technological cloud settings. Fulfilling IAM criteria enables the principles of least privilege and role-based access management. Furthermore, the IAM domain includes technical and organisational requirements for ensuring that appropriate individual network entities, such as users and devices, have access to the appropriate resources at the appropriate times and for acceptable reasons.

- Interoperability and Portability
  The Interoperability and Portability (IPY) domain comprises 4 control requirements. The necessity that the components of a processing system operate together to get the desired outcome is known as interoperability.

- Infrastructure and Virtualization Security
  The Infrastructure and Virtualization Security (IVS) domain assists CSPs and CSCs in putting controls in place to protect infrastructure and virtualization technologies. The IVS domain's 9 controls encourage the creation and maintenance of policies and processes for proper planning, securing, and improving infrastructure resilience, as well as the use of virtualization technologies.

- Logging and Monitoring
  Security operations rely heavily on logging and monitoring. The 13 controls in this domain are focused on governance and procedure, giving cloud-based businesses the tools they need to achieve effective logging and monitoring.

- Security Incident Management, E-Discovery, and Cloud Forensics

The Security Incident Management, E-Discovery, and Cloud Forensics (SEF) domains have 8 control requirements that guarantee that specified policies and procedures are followed to appropriately respond to security incidents and manage business risks.

- Supply Chain Management Transparency and Accountability
  The Supply Chain Management Transparency and Accountability (STA) domain defines a wide range of risk management procedures for supply chains. There are 14 control standards in the STA domain.

- Threat and Vulnerability Management
  The Threat and Vulnerability Management (TVM) domain has 10 control specifications that cover a wide range of concerns that could evolve into long-term difficulties with an organization's infrastructure's security architecture and engineering. Assessing and managing vulnerabilities that may evolve and damage assets, security architectures, designs, and solution components is the emphasis of this domain.

- Universal Endpoint Management
  The Universal Endpoint Management (UEM) domain is concerned with putting controls in place to reduce the dangers of using a computer outside of the office, including mobile devices and endpoint devices in general. The UEM domain aids organisations in applying 14 control requirements successfully.

IV. CLOUD CONTROL MATRIX FOR EFFECTIVE RISK, THREATS, ATTACKS, AND VULNERABILITY MEASUREMENT

To assess the effectiveness of security controls, 26 risks, threats, attacks, and vulnerabilities from Table I were mapped onto the CCM. Risk, threat, attack, and vulnerability were chosen from the list during the mapping process, and then descriptions of each control were read. The security controls of CCM that can reduce risks were chosen and then thoroughly analysed to see if the selected controls have sufficient measures to mitigate or partially mitigate the risk, danger, attack, or vulnerability. We follow since it offers implementation instructions for the control specifications for each of CCM v4.0's 17 cloud security domains, which are taken into account when mapping the 197 security controls.

Table II shows the domain name with the control number and a detailed description of how to reduce and mitigate risk, threats, attacks, and vulnerability.

Table III shows the details of the selected security controls against each risk. Every risk, threat, attack, and vulnerability solution mapped in CCM is either active or inactive. If it's there, we'll make a green tick mark, and if it's not, we'll make a blank box. If a tick appears, we count how many solutions there are in the 26 categories of risk, threats, attacks, and vulnerability.

TABLE III. CLOUD RISK, THREAT, ATTACK, AND VULNERABILITY MAPPED ON CLOUD CONTROL MATRIX

	Risk, Threat, Attack and Vulnerability	**Cloud Control Matrix**																
		(A&A)	(AIS)	(BCR)	(CCC)	(CEK)	(DCS)	(DSP)	(GRC)	(HRS)	(IAM)	(IPY)	(IVS)	(LOG)	(SEF)	(STA)	(TVM)	(UEM)
1.	Backdoors				✓			✓									✓	
2.	Formjacking					✓												
3.	Cloud Cryptojacking					✓	✓		✓			✓			✓	✓		
4.	DNS Poisoning Attacks							✓			✓			✓				
5.	Drive-by Downloads			✓			✓						✓			✓		✓
6.	Exploits and Exploit Kits		✓						✓							✓	✓	
7.	Data Breach	✓				✓	✓										✓	✓
8.	Log4Shell					✓	✓							✓			✓	
9.	Social Engineering				✓		✓			✓				✓				
10.	Cloud Provider Malicious Insiders						✓				✓				✓	✓		✓
11.	SQL Injection Attack				✓	✓	✓											✓
12.	Man in the Cloud Attack		✓								✓			✓				
13.	Operational Technology (OT)		✓		✓													

14.	Zero-Day Attacks	✓																
15.	Pixel Flood Attack						✓											
16.	Server-Side Request Forgery (SSRF)				✓								✓		✓			
17.	Deepfake Attacks			✓						✓								
18.	Insider Attacks	✓																
19.	SaaS Layer Attacks			✓					✓						✓			
20.	PaaS Layer Attacks			✓					✓						✓			
21.	IaaS Layer Attacks			✓					✓				✓		✓			
22.	Cloud AI Powered Attacks										✓			✓	✓			
23.	VM Scheduler based Attacks												✓					
24.	Cloud Phishing Scams		✓								✓			✓	✓	✓	✓	
25.	Crypto Cloud Mining					✓						✓			✓	✓	✓	
26.	Absence of Cloud Security Architecture and Strategy		✓	✓					✓	✓				✓	✓	✓	✓	

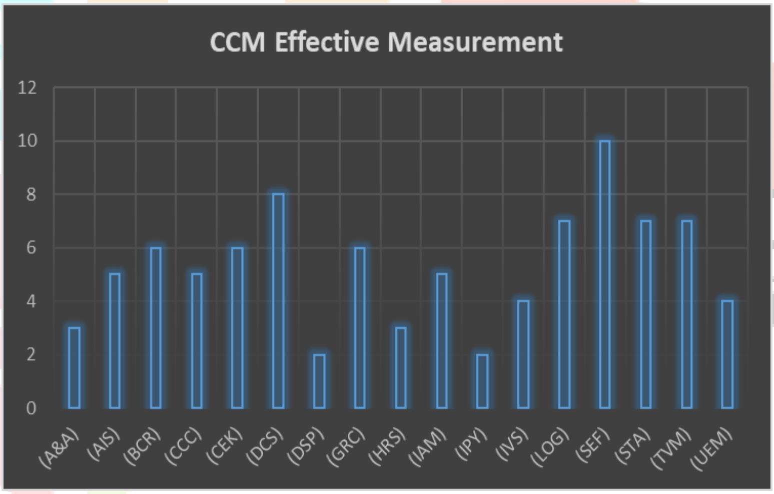

Fig. 6. Cloud Control Matrix Chart

All Security Incident Management, E-Discovery, and Cloud Forensics (SEF) is the most effective domain of the CCM, according to an in-depth review of the domain and controls, and enterprises are required to apply controls in the ibid domain more thoroughly. The Datacenter Security (DCS) domain of the CCM is also the most effective, as it deals with moving software or data/information to an offsite or alternate location, as well as maintaining and operating the data centre. Logging and Monitoring (LOG), Supply Chain Management, Transparency, and Accountability (STA), and Threat and Vulnerability Management (TVM) are the most commonly used domains, according to effective measurement. Business Continuity Management and Operational Resilience (BCR), Governance, Risk Management and Compliance (GRC), and Cryptography, Encryption, and Key Management (CEK) are therefore useful in mitigating identified risks.

Furthermore, it demonstrates that when implementing CCM in an organisation, organisations should concentrate on the Identity and Access Management (IAM), Application and Interface Security (AIS), Infrastructure and Virtualization Security, Universal Endpoint Management (UEM), and Change Control and Configuration Management (CCC) domains.

The quantitative study should show that CCM is capable of addressing cloud-related security problems for cloud suppliers, cloud organisations, cloud customers, and cloud providers. Furthermore, any security risk, danger, attack, or vulnerability that is not totally mitigated by the CCM implementation can be neutralised by the implementing controls. It's vital to realise that not every risk, threat, attack, or vulnerability needs to be addressed owing to cost. Various risks, threats, attacks, or vulnerabilities are less harmful, but mitigation costs are significant; such risks, threats, attacks, or vulnerabilities are decreased when a security framework is used.

V. CONCLUSIONS

This article focuses on understanding the various types of risk, danger, attack, and vulnerability that frequently appear in cloud computing systems. In this work, we attempt to present an approach that contributes to identifying risk, danger, attack, or vulnerability categories based on cloud service resources. With the rapid advancement of information technology, particularly cloud computing technology, it is probable that once a sort of danger or assault in the cloud computing environment has emerged, it will continue to proliferate, necessitating early detection. The Cloud Computing Model (CCM) is one of several cloud computing recommendations produced by the CSA. CCM is a security architecture that addresses risks, threats, attacks, and vulnerabilities associated with cloud computing. Some cloud organisations are now using the CCM to meet security requirements.

To distinguish risks, dangers, attacks, or weaknesses associated with distributed computing that are oftentimes featured by cloud associations and scientists, an orderly writing audit approach was utilized. For every space of the CCM and its going with controls, the productivity of the controls just as the area of the CCM were researched. Each danger was looked over the list throughout the mapping process, and 197 security controls were assessed to determine if they minimised the risk, threat, attack, or vulnerability.

Following that, a list of related CCM controls, as well as the mitigation degree of those controls, were chosen for each risk. According to the analysis, the most effective domains of the CCM for managing cloud-related risks are SEF, DCS, LOG, STA, and TVM. Cloud businesses must pay great attention when adopting these domains into their operations.

REFERENCES

[1] Abdurachman, E., Gaol, F. L., & Soewito, B. (2019). Survey on threats and risks in the cloud computing environment. Procedia Computer Science, 161, 1325-1332.

[2] Amuthan, A., & Sendhil, R. (2020). Hybrid GSW and DM based fully homomorphic encryption scheme for handling false data injection attacks under privacy preserving data aggregation in fog computing. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5217-5231.

[3] Kholidy, H. A. (2021). Detecting impersonation attacks in cloud computing environments using a centric user profiling approach. Future Generation Computer Systems, 117, 299-320.

[4] Li, L., Wang, X., Xia, Y., & Yang, H. (2019). Predictive cloud control for multiagent systems with stochastic event-triggered schedule. ISA transactions, 94, 70-79.

[5] Bokhari, M. U., Makki, Q., & Tamandani, Y. K. (2018). A survey on cloud computing. In Big Data Analytics (pp. 149-164). Springer, Singapore.

[6] Moravcik, M., Segec, P., & Kontsek, M. (2018, November). Overview of cloud computing standards. In 2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 395-402). IEEE.

[7] Malik, M. I., Wani, S. H., & Rashid, A. (2018). CLOUD COMPUTING-TECHNOLOGIES. International Journal of Advanced Research in Computer Science, 9(2).

[8] Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2019). Systematic identification of threats in the cloud: A survey. Computer Networks, 150, 46-69.

[9] Abdurachman, E., Gaol, F. L., & Soewito, B. (2019). Survey on threats and risks in the cloud computing environment. Procedia Computer Science, 161, 1325-1332.

[10] Prasad, C. S. S., Yadav, B. P., Mohmmad, S., Gopal, M., & Mahender, K. (2020, December). Study of threats associated with cloud infrastructure systems. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022055). IOP Publishing.

[11] Devi, B. T., Shitharth, S., & Jabbar, M. A. (2020, March). An Appraisal over Intrusion Detection systems in cloud computing security attacks. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 722-727). IEEE.

[12] Singh, V., & Pandey, S. K. (2020). Cloud computing: vulnerability and threat indications. In Performance Management of Integrated Systems and its Applications in Software Engineering (pp. 11-20). Springer, Singapore.

[13] Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[14] Khan, N., & Al-Yasiri, A. (2018). Cloud security threats and techniques to strengthen cloud computing adoption framework. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 268-285). IGI Global.

[15] Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., ... & Shen, H. (2018). A manifesto for future generation cloud computing: Research directions for the next decade. ACM computing surveys (CSUR), 51(5), 1-38.

[16] Bokhari, M. U., Makki, Q., & Tamandani, Y. K. (2018). A survey on cloud computing. In Big Data Analytics (pp. 149-164). Springer, Singapore.

[17] Jyoti, A., Shrimali, M., Tiwari, S., & Singh, H. P. (2020). Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4785-4814.

[18] Gong, X., Chen, Y., Wang, Q., Huang, H., Meng, L., Shen, C., & Zhang, Q. (2021). Defense-resistant backdoor attacks against deep neural networks in outsourced cloud environment. IEEE Journal on Selected Areas in Communications, 39(8), 2617-2631.

[19] Murugesan, S. (2019). The cybersecurity renaissance: security threats, risks, and safeguards. IEEE ICNL, 14(1), 33-40.

[20] Jayasinghe, K., & Poravi, G. (2020, January). A survey of attack instances of cryptojacking targeting cloud infrastructure. In Proceedings of the 2020 2nd Asia pacific information technology conference (pp. 100-107).

[21] Berger, H., Dvir, A. Z., & Geva, M. (2021). A wrinkle in time: a case study in DNS poisoning. International Journal of Information Security, 20(3), 313-329.

[22] Genkin, D., Pachmanov, L., Tromer, E., & Yarom, Y. (2018, July). Drive-by key-extraction cache attacks from portable code. In International Conference on Applied Cryptography and Network Security (pp. 83-102). Springer, Cham.

[23] Hopkins, M., & Dehghantanha, A. (2015, November). Exploit Kits: The production line of the Cybercrime economy?. In 2015 second international conference on Information Security and Cyber Forensics (InfoSec) (pp. 23-27). IEEE.

[24] Ezhilarasi, T. P., Kumar, N. S., Latchoumi, T. P., & Balayesu, N. (2021). A Secure Data Sharing Using IDSS CP-ABE in Cloud Storage. In Advances in Industrial Automation and Smart Manufacturing (pp. 1073-1085). Springer, Singapore.

[25] MICHAEL GORELIK (2021) CYBERSECURITY NEWS, THREAT RESEARCH, AND MORE FROM THE LEADER IN MAKING BREACH PREVENTION EASY.

[26] Alharthi, D., & Regan, A. (2021, January). Social engineering InfoSec Policies (SE-IPs). In the 14th International Conference on Network Security & Applications (CNSA 2021). CICT (pp. 521-541).

[27] Verizon (2021) Data Breach Investigations Report (DBIR).

[28] Xiao, F., Zhijian, W., Meiling, W., Ning, C., Yue, Z., Lei, Z., ... & Xiaoning, C. (2021). An old risk in the new era: SQL injection in cloud environment. International Journal of Grid and Utility Computing, 12(1), 43-54.

[29] Mupila, F. K., & Gupta, H. (2021). A Multi-factor Approach for Cloud Security. In Innovations in Computer Science and Engineering (pp. 437-445). Springer, Singapore.

[30] Holmström, A. (2021). Applying information security to the operational technology environment and the challenges it brings.

[31] Rana, S., Hossan, M. A., & Adel, A. (2021). Cloud Zero-Day Attack Detection Using Hidden Markov Model with Transductive Learning.

[32] Jain, H., & Saxena, A. (2019). Result Analysis of Existing Cloud Security Models.

[33] Jabiyev, B., Mirzaei, O., Kharraz, A., & Kirda, E. (2021, March). Preventing server-side request forgery attacks. In Proceedings of the 36th Annual ACM Symposium on Applied Computing (pp. 1626-1635).

[34] Abdullayeva, F. J. (2021, October). Detection of Cyberattacks in Cloud Computing Service Delivery Models using Correlation based Feature Selection. In 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-4). IEEE.

[35] Jacob Serpa (2019) Prying Eyes Inside the Enterprise: Bitglass' Insider Threat Report.

[36] Priya, A. (2021). A Detailed Survey Of The Security Issues And Defensive Tactic In Cloud Background. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(12), 2526-2532.

[37] Wu, Y. (2020). Cloud-edge orchestration for the internet-of-things: Architecture and ai-powered data processing. IEEE Internet of Things Journal.

[**38]** Mandal, S., & Khan, D. A. (2020, September). A Study of security threats in cloud: Passive impact of COVID-19 pandemic. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 837-842). IEEE.

[39] Kumar, R., & Goyal, R. (2021). Top Threats to Cloud: A Three-Dimensional Model of Cloud Security Assurance. In Computer Networks and Inventive Communication Technologies (pp. 683-705). Springer, Singapore.

[40] Cloud Controls Matrix Working Group (2021). CCM v4.0 Implementation Guidelines.