An Interpretive Analysis of Security Parameters in Cloud Computing

Ankush[1], Saloni Manhas[2]

Department of Computer Applications

Chandigarh School of Business

Chandigarh Group of Colleges, Jhanjeri, Mohali, India

amalik592002@gmail.com[1], salonithakur786@gmail.com[2]

Abstract:

In recent times, cloud computing has caught a lot of attention based on its low cost and excellent services. People and businesses cannot do without cloud services as they become more and more incorporated into the courses of their daily lives, as it has become over the past decade. On-demand pay-per-use features that outsourced manufacturers have the impact to speed up services and raise the value proposition. Beginning in 2022 cloud setup has become a trend and will be a growing trend for the coming years. Although cloud computing provides a wide range of benefits to both private users and business entities, data security problems are believed to be the strongest challenge to this technology in 2024. Whilst the factors of security are very many, cloud computing is no exception because of virtualization and multitenancy, as well as other features of on-demand. With that, the technology introduces new security gaps for malicious activities. To determine the current status in the area, researchers on service-based cloud computing safety problems in this paper. First, this paper deals with a cloud security analysis over the last decade and then a uniform security taxonomy across the mentioned three-layer model—IaaS, PaaS, and SaaS—is provided.

Keywords: **Cloud Security, Cloud computing, Encryption, Cyber Security, Cloud Environments, IaaS, PaaS, SaaS**

I. INTRODUCTION

These last ten years brought considerable development in the cloud technologies marketplace because the number of service providers and opportunities doubled; however, centralized data centers were replaced by decentralized ones. This occurrence gives rise to two related questions - what is the specific advantage of such infrastructure and how will it affect computers in the future? Certain services, motion, autonomy, data processing, connectivity, and self-management will be influenced as well as other things. Also, underlying concerns for such cloud systems of the future are realized with the cloud data rap.[1] To give relevant information to stakeholders of a variety of natures, the study addresses Latvian SMEs' cloud computing experiences and also looks at whether there is a correlation between performance indicators and pre-, and post-cloud migration.[2] The fact that pay-per-use cloud computing is in demand among both individuals and businesses proves that its sphere of application is vast as well as versatile. It attracts a larger audience of users due to the creative approach to the income.[3]-[5]

The NIST developed a concept of the service-based paradigm for cloud computing standards. In this model, which defines all ICT sharable resources including software, hardware, or networks, IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), and SaaS (Software-as-a-Service) are the most recognized cloud computing services.[6]-[7]

In this paper we study the the latest cloud computing security issues examine them and sort them out using a service-based taxonomy The main focus of this research paper is described in the details below.

1) Operating systems' vulnerabilities become more prevalent due to employing all of the cutting-edge cloud services.

2) Cloud services are facing the same taxonomy of countermeasures and vulnerabilities.

3) Trends in research together with the limitations in research are also identified.

4) vulnerability and countermeasure taxonomy has been developed.

5) A bullet list of the most prominent security pitfalls that the service-oriented paradigm has is compiled in the following table:

The article's remaining sections are arranged as follows:

The relevant conceptual notions serve as the basis of the discussion (Section 2). The upcoming paragraphs in section 3 address the current research condition. Sect., 4 and 5 point out the existing obstacles and the future research theses as well. The article explains the end of these two sections as Conclusions and Cue, respectively.

II. CLOUD COMPUTING OVERVIEW

A summary of this section is represented by the technologies as well as ideas of the service-based model which are described concerning the study topic. NIST addresses cloud security concerns based on three key categories: quality attributes, deployment model, and service-based model [3].

A. Cloud Computing Enabling Technologies:

The elementary principles like virtualization, multitenancy, and service-oriented architecture (SOA) have been crucial in the cloud computing development journey.[9] These approaches are physical examples and they promote the sharing of resources across users. [8]

1) Virtualization:

In the cloud, resource partitioning is being provided by virtualization, as the natural way assets can be managed on a virtual basis. Using a file often abbreviated as an image and can either be a personally created image or acquired from outside sources, sharing resources is made possible with the file use of a virtual machine [10], [11]. Virtually all IT resources which in principle become sharable can be virtualized to allow many users access through a single instance of each resource. The virtualization types that are widely exploited nowadays are desktop, network, storage, data, application, CPU, and cloud. Resources are virtualized and this virtualization exists through the IaaS, PaaS, and SaaS models [12–14]. A cloud computing service is illustrated using a graphic shape in Figure 1. The utility of a hypervisor is whereby the multiple levels of users receive slices of the same physical resources being allocated.

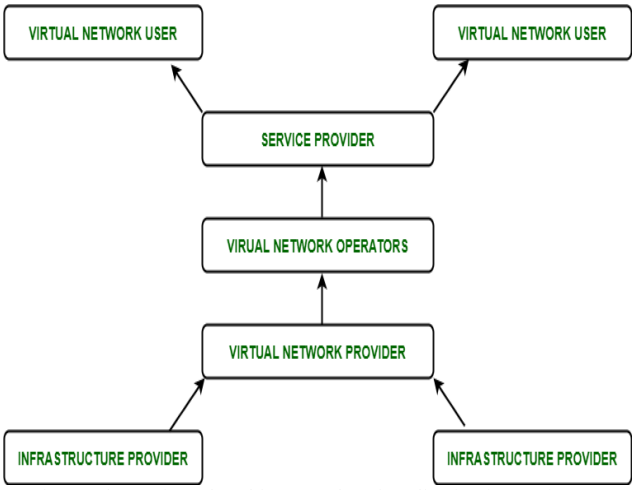

Fig. 1: Abstraction of Multitenancy by Virtualization in Service-based

2) Hypervisor:

VMMs are a product of fulfillment of very specific needs, as touched on, and trace their history to the 70s. For example, VMMs nowadays let us make most of the latest CPU releases which get better each time.[15] Nowadays it's becoming more commonly used to call them Hypervisors; the name Virtual Machine Monitor is losing its popularity.

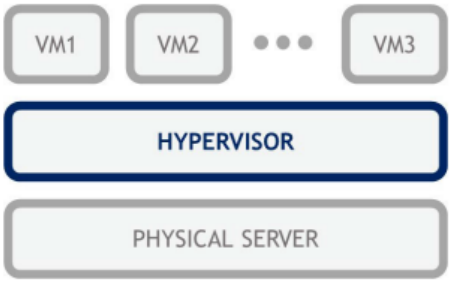

Fig.2: Hypervisor representation

The operating environment will split hypervisors into two types.

1. Type I hypervisors which are also known as bare-essence hypervisors work by placing the hypervisor on top of the host tackle. This translates to no operating system running below the hypervisor,[16] which acts as a scheduler and allocator of system coffers for each of the virtual computers.

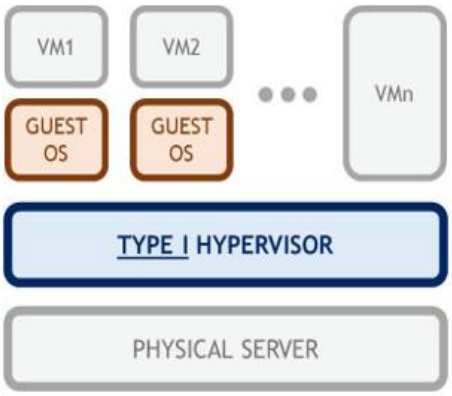

Fig.3: Type1 hypervisor

2. Type II Hypervisors are applications running on top of the host operating system. Because it works as the other process, the host operating system does not need to be informed.[17]

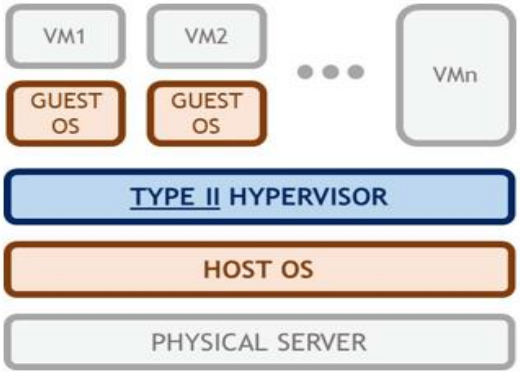

Fig.4: Type2 hypervisor

3) Multitenancy:

The fact that multiple clients can access the same instance of an application at the same under the concept of multitenancy simultaneously is one of the key benefits of software as a service. This approach gives users services by starving a few virtual machines (VMs) in a single server to share the computing power, memory as well as storage among them. By interconnecting different layers of systems like simple Object Access Protocol (SOAP) and HTTP, a Service–Oriented Architecture (SOA) realizes its service commitments to diversified client groups. This situation of multitenancy precisely conveys the scenario in Figure 1, which depicts the result of resource virtualization. Real machines like CPU and memory are virtually shared and assigned to multiple users with minded physical distribution of clients in the implementation of the multitenancy environment. However, creating a single instance results [18] in highly-optimized resource use that in turn, shared resources will be exposed to concurrent access that will cause the degradation of their performance.

4) Service Oriented Architecture:

A multi-tenancy architecture is the technical foundation upon which software as a service is designed and implemented. It is the reservoir of the many positives that customers can use the same instance of an app at a time. This is by way of the mechanism where the shared computing power, storage, and memory of one physical machine is allocated to each of the virtual machines and only when the requirement arises do the allocations begin. Hence, SOA achieves its goal that "systems rely on each other for shared processes" by SOAP and HTTP interconnections among the systems layer. This concept can be identified as IaaS principal characteristics and is described as the outcome in chart 1 above, which demonstrates the resource virtualization effect.[12] This does translate into real machines that combine a CPU and a memory and are then distributed amongst multiple users who physically are substantially apart. This makes certain environments virtual, a kind of multitenancy. Nevertheless, in the face of a place where only one version can be chosen, it will be more efficient of resources allocated which in turn will be a cause of their degradation of performance in sharing resources.[20]

B. Service-based Cloud Computing:

A technology that, instead of relying on a central server or a personal computer, stores, handles, and processes data on an Internet-hosted net of remote servers, is called cloud computing. Such distributed computing services are offered by businesses known as cloud service providers,[6], [7] and the prices are most of the time pay-as-you-use based. Building cloud computing on a grid or a cluster is business as usual.[12]

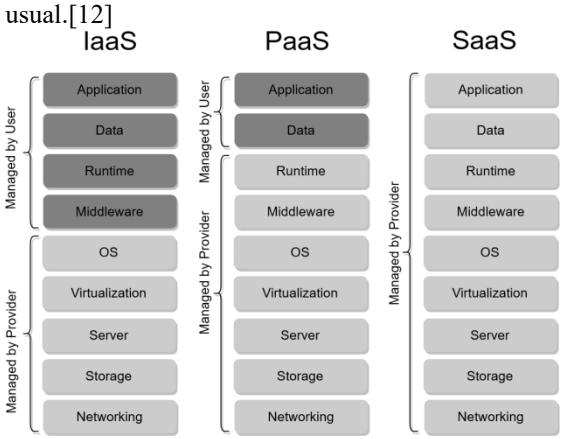

Fig.5: Resource Management in the IPS Model [12]

1) Infrastructure-as-a-Service:

The systems and the hardware are available across the board to the users in the form of networks, storage, compute power, etc. The user may run the software, together with the operating system and the apps, at the top of them. On the other hand, users have full control over operating systems, storage, and applications, but they might not have the ability to manage or control the predetermined components (such as host firewalls) however have no say in the underlying cloud infrastructure. IaaS is to build a set of computing infrastructure at the platform virtualization level which includes raw storage and networking and is presented in the form of services according to the definition of Cloud Security Alliance (CSA), a standard organization for cloud security setting.

Rather than getting data center space, software, or servers, we offer a turnkey solution that provides readily available computational resources, leaving the users free from some operational issues they will use internet access to lessen their expenses on network infrastructure.[22],[23]

2) Platform-as-a-Service:

PaaS is defined by the CSA as PaaS is defined by the CSA as: an infrastructure platform and solution stack being offered on a need-based model. With the aid of PaaS services, application deployment is much easier and the developer will not have to make too many purchases for the hosting of hardware and software part.

The CSA is saying that fact is real when you are accessing PaaS services you can only access online. PaaS vendors look into the application platform and grant programmers the leeway to use the tools at their disposal, which in turn, enable developers to perform tasks in a less complex manner. Thus, PaaS providers however demand the developers to work with what they offer i.e. the tools and software stacks they provide take away some space for flexibility.[21] However, at a lower level of software development, the developer (s) have very slim potency in parameter determination, viz. memory allocation and stack configurations (e.g., number of threads, cache size, patch levels, array size, etc)

This time

The majority of sophisticated PaaS solutions include the following sorts of extensions, as examples:

- Database
- Logging
- Monitoring
- Security
- Caching
- Search
- E-mail
- Analytics
- Payments

3) Software-as-a-Service:

A complete application provided as a service to a subscription user is called SaaS. Only the configuration of users and parameters that apply to particular applications remain for the service user to handle. The infrastructure, application, deployment, and all aspects of the service delivery are maintained by the service provider. Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Payroll, Accounting, and other routine business software such as SaaS applications which are frequently utilized. SaaS solutions are often used for non-core functionality. Companies choose to outsource SaaS for non-core business activities to save on hiring people who can maintain and support the product infrastructure. Besides, they pay for their membership and make use of online platforms only as they wish.

The software having lower costs means that the clients pay less than they would in the event of a license arrangement, and providers would attract more clients. They are being provided by innovators such as Google, Microsoft, and Amazon, including Google Drive, Microsoft 365, and Amazon AWS. [24-25]

C. Cloud Computing Management:

Management, therefore, begins to briefly explain another meaningful concept that is also essential in each of the SMEs' growth strategies and to help them become successful entrepreneurs in the future. Nine layers comprise a cloud computing architecture: hypervisors, network, storage, servers, midd/ware, OS, data, and application. The Common Accession Schema is the label given to this schema. One or several entities may be found to be running the managerial function of the layers of the service model. IaaS outsources the CSP a subset of the responsibilities such as networking, storage, servers, virtualization, and OS. Whereas, the end user is only responsible for the middleware, runtime, data, and applications. The entire stack-less PaaS came into existence when the user had control only of the data and application layers. However, the CSP handles everything else under its control. While with SaaS customers have decentralized decision power with suppliers being the main ones who take care of each layer of the cloud.[26]

D. Deployment Model

The exclusive access to the shared resources is set by the deployment model. Although private cloud computing provides organizations with unlimited access to their resources, public clouds make resources available to the general public over the World Wide Web. This approach enables the client to control the administration or the CSP to administrate the services. Also, the infrastructure might be located at the CSP site or could be operated by a private host.[27] A community model would be a suitable way to access cloud services for customers who are concerned with security concerns. Even though done by the organization for a customer to acquire services from other organizations, the management and resource access are comparable to the private model. When two or more models of deployment are put together, it leads to a hybrid model.

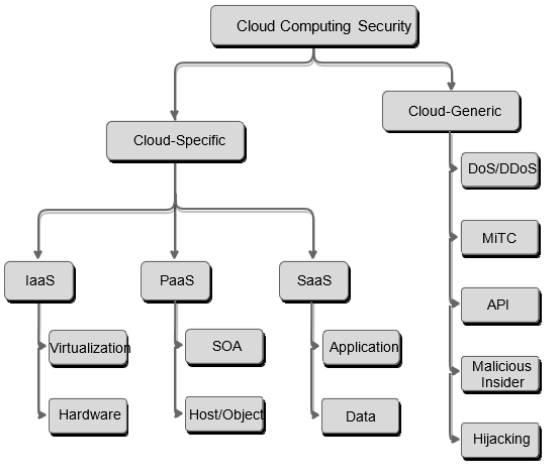

Fig. 3: Cloud Computing Security Taxonomy

III. RECENT ADVANCES IN CLOUD COMPUTING SECURITY

The most elaborated topics in cloud computing security literature, which are almost the same as one another in their tools, strategies, privacy, and policy considerations, are virtualization, multitenancy, data security, and general vulnerabilities, but researchers have examined the security challenges of cloud computing from different perspectives. By the security issues mentioned above, this paper discloses the security taxonomy which is the important topic of this study. Cloud attack security taxonomy is broadly divided into cloud-specific and cloud-generic categories under which specific classes of cloud vulnerabilities are centered. An enterprise service bus, a platform as a service (PaaS), software as a service (SaaS), and other specialized service issues are addressed by the first.

A. Cloud-Specific

Technologies, as well as concepts such as virtualization and multitenancy that make up the cloud architecture, should be at the disposal of the cloud infrastructure. The client segment is with the business model of IaaS, PaaS, and SaaS which are delivered by different means. The same technology could be the cloud solution tipping point of the operation of the cloud environment. This section contains the items that are most often discussed as security vulnerabilities and corresponding security fixes in the academic community.

1) IaaS

In the service provided by IaaS (Infrastructure as a Service), consumers are promised the virtualized physical equipment as a service. The idea of virtualization is the starting point for the majority of the significant safety pitfalls in this layer. The top security vulnerabilities to be taken into account at this level are those of hardware, virtual devices, HV, and VM images [28].

We illustrated the vulnerabilities of IaaS layers and corresponding mitigation strategies.

i. Virtualization

The VM images that are mainly targeted by the attackers are files that come with VM configurations and log files that are used in VM operations. Certain types of morphing through picture templates may lead to data breaches and injection code photo manipulation [29]. Gonzalez studied four IaaS architectures with diverse security parameters, which include [30]. The most effective architecture is considered to be a sequence of crypto-protecting, access control, signature policy, and isolation. This model is indeed secure as it implements different encryption methods to protect the VM images, but once a live VM is infected using attacks such as disk injection, side-channel, VM CPU timing, and HV-based attacks, a potential compromise may happen. The mentioned problems can be alleviated through the usage of the Bayesian network technique. According to this particular method, there exists a trust zone faceted by interconnected components.

Zhang et al. analyze security threats dealing with AMI in AWS on the Amazon EC2, and the security

flaws in AMI (Amazon Machine Image) [21]. The risk-gain value of any vulnerability is calculated using the mathematical model. This can be done with tactic-game modeling, which is a subset of system modeling. For this scenario, the sooner the responding element gets to the battlefield, the better the effect it can have. The poll concluded that the Ubuntu operating system is the attacker's preferred O/S in 50 percent of attack execution hence the attacker attack pathway perfectly. The chances of a DoS attack are higher because an inappropriate configuration of the virtual machine image also leads to DoS vulnerability. Nevertheless, the feasible workaround is to make sure all versions are kept up to date, unexceptionably conversely this is a tough task. In addition, a few valuable details on the solution of VM image issues are covered like patching a public VM image, maintaining the working instances, prioritized vulnerability patching, and defensive cloud infrastructure rearrangements.

The "VM escape" vulnerability provides an attacker with the capability of speaking directly to the host operating system beyond a hypervisor and once this is done, the said attacker will have the root privileges. Three countermeasures are presented to address the VM escape problem: HyperSafe, Trusted Cloud Computing Platform (TCCP), and Trusted Virtualized Datacenter (TVD). HyperSafe later enhances its security to block write-protected memory changes hence stopping hypervisor bypassing. The technique isolates the execution environment through TCCP. This notion involves a TC and a TVMM that are maintained by a TTP. The role of the latter is at the center stage. The TVD technique virtually clusters a computer's user into groups based on their interests. The following step is the securing of communication channels which is done to protect all the communication that happens among the groups [31].

Through the common use of environments, the HV achieves the concept of multitenancy. HV is a target of intrusions because privileged access is easy. If the HV is successfully breached, then the attacker fires all kinds of attacks, including rootkit and kernel structure manipulation. A hardware security solution called the Trusted Platform Module (TPM) utilizes hardware features to ensure the security of the components such as power supply units and circuit boards. This method named BIOS signature is used by the technology for providing a secure boot time. In modern hardware processors' crypto chips, the latency of a secure startup time and HV tampering blocking are features. Among other tests, the processor executes the boot-time software to authenticate the data [30].

ii. Hardware

To enhance the privacy of data while being transmitted and stored, cryptography techniques are applied. Regardless of how strictly the safeguards work, data has to be eventually decrypted for operational purposes. Thanks to cloud multitenancy capability, access to storage media such as disk, RAM, and cache is getting more readily. The value of the key of any type of sensitive data that is saved in storage media, meanwhile, is accessed by intruders who are sharing a host with the victim. A type of such problem is illustrated by cache-based side-channel, a family of cross-VM side-channel vulnerabilities. The limitation of the above-layer users' access to below layers is another contentious issue associated with cloud-based services. Software Guard Extension (SGX) is the technology developed by Intel to provide memory protection. node where the enclave, or application, is hosted. The OS is also restricted from accessing this area in the secure enclave [32].

2) PaaS

Under this layer, clients are given access to all the essential services through SOA way of deployment requirements. Security issues become more probable with the sharing of resources by multitenancy and SOA [33]. The vulnerabilities related to the PaaS layer with the corresponding patch indicated.

i. SOA

Competition of interests for customers among the parties involved in a common enterprise results in resource management difficulties. The colocation of two adversaries at the same host is considered an example of this. The Chinese Wall Model gives each user a specific conflicting organizational area and ensures the distribution of physical resources and thus resolves the problem of unintended or intentional sharing of shared resources. An integration approach could be used where, policies, monitoring, and constraints are resolved with multi-tenancy and virtualization. The SLA (Service Level Agreement) is one of the statements that makes clear how resources will be distributed between the parties and what roles and functions are expected of each. Yet another policy that supports this is known as the Secure Configuration Policy (also abbreviated as SCP), which guarantees that the local layers of the hardware/software or SLA configurations are fully secured.

In the cloud services context, Freet et al. [47] show the impediments to digital forensic security.

Concerning this way of thinking, the IaaS tier is essential for the provision of shared resources such as CPU power and data storage. The packets of a virtual machine communication are sent through a host device in different directions across a shared resource area. The VM isolation still allows for VMs to be compromised inside the company. Subsequently, these malicious VMs are capable of attacking other VMs within the organization. In addition, if the HV is misconfigured, one virtual machine can use all of the framework resources in a shared environment and do the denial-of-service to another virtual machine. Sneaky intentions can affect the PaaS layer and corrupt the whole infrastructure of the cloud. Rather than PaaS the SaaS model comes with a service-oriented architecture, and its main security risks include injection, DDoS, XML-related, and, MiTC attacks.

ii. Vulnerable Host/Object

Apart from the roommates, the hosts and other strangers can come around without any clear indication. As such, their belongings are always at risk of being stolen or damaged accidentally. One of the major issues is providing secure objects as well as coordination between in-API connections; therefore, the combined TCB is widely used [53]. on the other hand, a model of 4 practices is being presented to deal with vulnerable items. ULP, or logging facility that can't do without, PEPs or enforcement policy, TLS, or security at the transport layer, and SACP, or a permanent access control policy, constitute the paradigm. The network protocol TLS has been adopted by a lot of people and has a cryptographic algorithm as its method of providing safe communication. ULP provides a validation of the systems logging system, while the SACP and PEP entail the object-based fine-grained access control [46]. The homogeneity of the function represented in cloud portals/platforms and APIs, considering they are all powered by the concept of interoperability, reflects PaaS' major weakness. TCBs target the issues of vulnerable hardware components by providing protection, as well as dealing with compatibility using a unified solution. The suggested solution could be enhanced by including the process of application encryption that will protect the items that are made public [50].

3) SaaS

SaaS uses a separate upper layer on top of two under layers, hence it inherits the vulnerabilities of the layers below. In addition, the model's working is based on online API and it is therefore vulnerable to technology-related attacks within the domain of this web [30]. To develop the overview of SaaS layer vulnerabilities alongside the remedies for each of them.

i. Application

OWASP's top 10 website technology vulnerabilities presented in this article are an empirical part of the mentioned gloss. The assurance of APIs on the web is undeniably in part defined by issues such as unsafe deserialization, cross-site scripting (XSS), injection, XML External Entities (XXE), vulnerable access control, accidentally exposed critical data, and insufficient logging and monitoring procedures [54].

The researchers Cohan, et al. [53] organize SaaS security issues problems into three sub-areas: applications, implementation, and data. Security bites consist of storing, transferring, backup, recovery, integrity, and access to data management. Using the internet, the projects and technologies are implemented. Application security involves user interaction, network traffic monitoring, protocol stack, code and data flow, and many other non-obvious factors. An online application's design and execution involve front-end and back-end programming languages including HTML, JavaScript, Python, Java, SOAP, PHP, etc. hence, focusing on style and functionality. A design in most cases leaves optimal security conception out and behaves more like vulnerability.

ii. Data

Nevertheless, great attention to the rule concerning data security is placed on all cloud tiers, whereby SaaS customers have to rely fully on the CSP as a gateway in cases of credential information breaches that may occur during transfer or storage. Digital signatures, homomorphic encryption, and FRS—"fragmentation-redundancy-scattering"—were proposed as the solution to the problem of data leakage which was described by Hashizume et al. [31]. The HRS headspace redundantly drives a fragment of the basic ski data around the system after it was cut up into pieces of minimized data. The RSA algorithm is involved in the digital signature method through which the authenticity of the data can be verified once the data is transmitted over the network. When the original message is transformed in the encrypted form; Homomorphic methods are to be applied. Among the many ways, the following one could play the role of it is decided depending on the goals of the system.

B. Cloud-Generic Vulnerabilities

The network technologies that have already inherent security flaws, for example, there is the vulnerability

of TCP/IP are the foundation of cloud computing [52]. Under this strategy, an issue will be raised between general and particular security problems. Whereas the previous one is related to network issues, in general, cloud-based problems affecting all levels or a filiation at a layer, such as virtualization in IaaS [32]. The cloud vulnerabilities and their mentioned workarounds are stated as common.

1) DOS/DDoS

The attacker capitalizes on a vulnerability of the Transmission Control Protocol in the Denial of Service or the Distributed Denial of Service attacks thus starving legitimate users of network bandwidth, CPU, or routers to crush or render his/her legitimate service inoperable. The cloud computer architecture VMs do not have enough bandwidth and therefore have to face a risk of DoS attacks. Some of the articles [41], and [48] provide a few tips that can limit the interaction with this bombardment.

DoS traffic is detected using establishing session limit and SYN cookie analysis. The process of SYN Flow analysis communication between client and server has the following dialogue which are synchro messages. The launching of the handshaking for synchronization is commenced by the attacker as in the SYN flood assault but it never finishes. Moreover, the server is warding off any possible acknowledgment communication being sent from the client, a crucial security factor for DoS attack prevention.

The final and concluding stage of the handshake operation will occur and all processes will commence once the right SYN-ACK is attained. However, it is the computer that is responsible for the synchronization rendering the TCP socket redundant and tricking the server to never have ever hosted the unfinished synchronization process. The next approach to creating of DDoS attack is to use open connections which require to be handled and maintained by resources thus keeping them busy. As a matter of rule, the drawback is usually avoided by IP address clustering that prevents connection shared by clients with the same IP address.

2) MiTC

The third danger that the generic category is exposed to is known as Man-in-the-Cloud (MiTC) attack where an intruder can begin by gathering information from the internet and identifying a potential victim. The attacker starts the malicious activity after getting a loophole(s) in the system, for example, open ports or unprotected servers. Consequently, a range of measures could be taken to minimize the chance of MiTC attacks [64], such as preventing probes with firewalls and intrusion detection systems, hiding sensitive data shutting down the ports, and blocking any sort of routing bypass. Moreover, the present ones serve to contain DoS attacks [48].

3) API

The common usage of API refers to the Application Programming Interface. The main drawback of this feature is the even more severe convenience encountered while combining data. In the absence of such a policy, incompatibility would get more entrenched in the artistic community and affect the majority of artists [46]. The customer is ensured that a server log system is centralized to record any suspicious action including spying or tampering to be able to help in the investigation. Following this, the encryption of the log file is carried out and it is signed for storage so that any attempt of modification can be avoided [47].

Zissis et al. have conducted an audit that focused on certification and authentication, which are important operations of an information system [9]. For example, granting permission covers the range from allowing hardware or software activation right through to preventing unauthorized use of the system. On the other hand, authentication confirms each user's identity. Shibboleth which is based on the open-source middleware standard SAML takes care of transmitting and authenticating the users.

4) Malicious Insider

Cloud computing employees who are collaborating with the inside threat to abuse their system access credentials can be defined as malevolent co-insider threats. The use of Mandatory Access Control (MAC) and Discretionary Access Control (DAC) are the two types of Control (such attacks from being opened up) [8]. Through the use of technical methods, the OS is configured to have a strong policy; an example is limiting access. Since MAC is known to raise the level of security, for the cloud environment it should be an appropriate access control tool. Showing among many techniques of the Pattern Matching concept, we can consider Trusted BSD in Mac OS and App Armor in Linux [32].

In [45], Kamongi and his colleagues introduced a methodology called VULCAN computer that is essentially a comprehensive security evaluation involving ontological reasoning and NLP or natural language processing for the assessment of security vulnerabilities in cloud computing systems (CCS). The platform checks the Ontology Vulnerability Database (OVDB) and National Vulnerabilities Database (NVD) repositories to define exploit

signatures, novel patterns, or known vulnerabilities used to gain access. A vulnerable database and an online vulnerability database are among the tools used by the framework to index every circulation of every possible vulnerability. Following that, the app will look into any potential security issues with a cloud-based system. Each vulnerability has a designated log which is organized into groups according to the VULCAN architecture paradigm, which is consistent with the rules of the classifier. The aptness of the design lies in the ability to use as a key feature of the vulnerability to determine, whether an alarm is henceforth respectively either about reaching a single known category or multiple known ones. A hurricane did not disable a polymer pathway which itself would lead to further harm as Gonzales and colleagues [30] employed a Bayesian network to identify bad paths.

5) Hijacking:

The stealing of credentials for user accounts as a pill can be used in furthering this foul play is represented by account or service hijacking. It is important to have reliable identity and access management guidelines to help in problem mitigation. Another shield against compromising devices is the application of rotational credentials. Depending on the previously determined parameters such as the user's location or the received items, the method amends the secret values previously saved [31].

Khan et al. [44] support their privacy and security points by interviewing cloud developers/providers as well as IT administrators about current and future contexts. If one of the tiers or stages is set in a way that differs from the appropriate activity or if a vulnerability is not configured correctly, it may become the source of a vulnerability. Settling on the primary cause of the problem will go a long way toward recognizing and stopping the hijacking by its trace. The final section is consistent with the above-mentioned findings about the lack of serious permission validations and weak credentials which are common reasons for an account or service to be stolen. Insecure platforms mishandle, inappropriately process, and safely store the data which can cause its leakage. The DoS attack is perpetrated more prominently if the third-party APIs are insecure. SQL injection or cross-site scripting can be used by attackers to get control of user data. Virtual machine network sniffing and spoofing attacks are more querulous on an unprotected virtual machine instead. If credentials like usernames and passwords are stolen to gain access to a system, then these kinds of accounts or service instances are hijacked. A “hoverboarding attack” can be performed from both tiers as the attack vector, in this case, is the cloud since cybercriminals now have more points of attack on the business systems. Cryptography techniques, NIDS, two-factor authentication, and PDP security systems are examples of countermeasures that can be adopted to avoid session or account takeover [55].

IV. CHALLENGES

Companies and people also can make big money from the concept of cloud computing. However, complex designs and applied technologies cause problems, this has to be overcome. SaaS, PaaS, IaaS, and common security issues have been the main topic of discussion.

A. IaaS Security Challenges

Research indicates that the biggest harms to the system as a whole are related to vulnerabilities at the lower levels. Hence, it is natural to assume that if the IaaS layer has a security flaw, it will spread throughout the multiple layers and eventually put the entire system at risk. The client is deprived of the capability to devise an efficient security countermeasure as the lower layers are not open for access [31]. The major security problems for this tier are multi-tenant and virtualization. Under provisioning of bandwidth or colocation VM escape can make virtualization in the IaaS context expose incidental security flaws, for example, DoS and cross-VM side-channel attacks [43]. While in an IaaS setup, there may be some vulnerabilities in VM images. That is where virtual machines (VMs) can be established, either by using a public or private image. Public pictures can be sent to external sources other people, open-source communities, and IT corporations. There are about more than six thousand public photos that can be used on Amazon EC2. Of course, the output of the recent research says that public photos can serve as a backdoor because their suppliers might not properly delete keys or other crucial data [44].

The hacker’s traditional attack entrance is network stability configuration. Contrasting to the IP address range of a traditional computer, which is less reliable and unpredictable, the IaaS layer is the majority of the time more reliable and predictable. Moreover, machines that are not connected to the cloud might resort to firewalls or other security solutions. The embedded nature of the ecosystem in the cloud makes it difficult to adjust.

B. PaaS Security Challenges

The one negative side of PaaS may be called the lock-in. The PaaS paradigm provides a way for software developers to customize and synthesize the available hardware resources and software to create a product in a flexible and scalable manner. The interoperability problem is very dangerous for PaaS customers because no one has been able to agree on the standards or the rules to be followed. An example of vendor lock-in happens when a client requires services, that aren't provided by the environment, established by the primary vendor [40]. This can be achieved by the client by changing a place of keeping or hiring a new provider. However, the deal of migration from servers of other vendors to mine is just like a waste of money and precious time. As a result, the customers of PaaS would find themselves at a lock-in point and have the risk of moving the environment to an alternative vendor by paying the price of migration or continuing with the service provider that has certain restrictions [41].

The shared environment of applications and software can be used by PaaS customers due to the application of the SOA concept. One of the benefits of the concept is that a PaaS implementer could not manage access to the lowest layer which hinders the implementation of security solutions. Hence, this system is prone to both injection and DoS attacks, in addition to Mixed Traffic and XML threats. This is mainly due to its initial configuration. One of the highlighted bullet points is that the PaaS API should also enforce high-security requirements for upper-layer clients who will be utilizing the services.

C. SaaS Security Challenges

Each one of the two parties, a person who uses or less expensive platform provider can benefit from the multitenancy. Users would be charged by the go in some cases but major online storage as Google Documents will remain conceded. This truth is sustained where multiple users can be in a system that possesses both software and hardware at the same time. Using such a transmission method would be troublesome when it comes to managing the data. In a system with different users, data-localization, integrity, confidentiality segregation, and backup would be difficult to maintain.API web services expose methods to the security vulnerabilities of web technology via the definition of SaaS delivery to customers for the circumstance of roommate living, a bad policy will lead to significant security or privacy problems, like data access in a roommate living arrangement and data leaks in a shared database system.

This gives another major problem related to the control limitation: a user in the cloud SaaS has no impact on the operating system, middleware, or application, while this user still has control over the user interface. This statement translates into the fact that customers may choose to use the application from the CSP only, which keeps all services. This prohibition or restriction should be neatly outlined so that the customer cannot seek log files or any other monitors, modifiers, or secure policy applicators.

D. Cloud-Generic Security Challenges

The release of software patches on a steady basis prevents risks from being exploited at all levels. Similarly, in the paragraph provided, it is clear that one of the vulnerabilities mentioned was the software's inability to timely patch up as well. The vendors reduce the risks of numerous security flaws by carrying out updated patches in a scheduled manner. Eventual consequences vary from people who take new updates seriously to those who are ignorant about them. Cost-effectiveness in a cloud environment is the issue that brings hackers' perspective and the users' perspective closer together. Attackers can effectively pass the penetration test if they use low-cost devices or hardware. This is what makes these cloud users vulnerable to hackers as they want to get the benefits of cloud users [22]. The reason for an API security risk may come from the fact that they are poorly designed. Interoperability refers to the ability of systems with different components or platforms to work together harmoniously than would be usually expected. This ability is embedded with a few functionalities, which consist of cross-provider migration and customer- or CSP-side service upgrades [42].

Internet security factors such as DoS, DDoS, MiTC, and account or service hacking can be attributed to the Internet IP protocol. Each of those disabilities can be attempted from any level of investigation. However, PaaS is the architectural model of choice because it is a more likely model in which the attack is to be launched at this layer than in the other two [28].

The most well-known security threat that originates from malicious insiders should be assigned more attention to address. The human factor in cybersecurity is extremely vital as around 70% of attacks are tied to human error in businesses stated Bouayad et al. [28]. Nevertheless, we still have a lot more to go through the work with SGX like tools that guide us in the right direction.

V. LITERATURE REVIEW

A. The paper titled "A Study on Cloud Computing Security Challenges" by Santosh Bulusu, and Kalyan Sudia defines a Due to the factor of cost-effectiveness and greater accessibility, cloud computing reinvents scientific computing. Highlighting the fact that there are no global security standards this study offers 43 security concerns and 89 solutions. Scholars will be provided with knowledge of interoperability techniques designed to revolutionize the future of cloud security while practitioners will apply the techniques that are identified.[34]

B. The paper titled "Cloud Computing Security: A Survey on Service-based Models" by Fatemeh Khoda Parast, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B. Kent, and Saqib Hakak defines security remains the supreme priority, and virtualization and multi-tenancy are a new kind of threat. This essay concentrates on the fast-evolving field of cloud computing security and highlights the crucial role cloud computing plays in modern businesses. Besides, it ensures a well-established taxonomy of security problems across IaaS, PaaS, and SaaS tiers that will be perfect for effective strategy creation.[35]

C. The paper titled "A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges" by Marya Ayoub Omer, Abdulmajeed Adil Yazdeen, Hayfaa Subhi Malallah, and Lozan Mohammed Abdulrahman defines the This article is intended to evaluate the present cloud security transformation, which was triggered by the COVID-19 pandemic lockdown that caused people to work remotely. However all the cloud advantages, cybersecurity attacks are increasing in their frequency. Through a systematic analysis of security risks and suggestions to enhance cloud architecture via smart research synthesis the complexity of this land is made clear.[36]

D. The paper titled "Cloud Security Service for Identifying Unauthorized User Behaviour" by D. Stalin David, Mamoona Anam, Chandraprabha Kaliappan, S. Arun Mozhi Selv, Dilip Kumar Sharma, Pankaj Dadheech and Sudhakar Sengan. In this research, we are considering the evolution of cloud computing with internet-powering and distributed networks to provide on-demand, scalable, and elastic IT services. It presents means to bypass reliable cloud services for authorization and authentication with the help of threat model security and multi-agent systems. This project aims to strengthen cloud security through innovative authorization and authentication methods.[37]

E. The paper titled "A Comprehensive Survey on the Use of Hypervisors in Safety-Critical Systems" by Santiago Lozano, Tamara Lugo, (member, ieee), and jesús Carretero,(Senior Member, IEEE) defines achieving a diversity of applications such as air and car industries, the article will give a holistic review of hypervisors as a kind of technology that, could be applied in developing virtual safety-critical embedded systems. Hence, it carries out a feature-by-feature comparison of the selected hypervisors and offers practicians a starting point to select the appropriate hypervisor. [38]

F. The paper titled "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey" by Waqas Ahmad, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil defines Cost-effectiveness and better performance become the new standards by cloud computing exhausting the typical processes through rationalizing, and streamlining conventional operations. Nonetheless, with new features coming up, security vulnerabilities were quickly exposed. The emergence of innovative techniques became essential when the classic funding options played no role with closed-type systems. Given the fact that cyber threats extend, several approaches have emerged to get the edge over cloud security concerns in recent times. However, there are still some gaps, especially in big data analytics and applying machine learning and deep learning for cloud security enhancement. Thus, advancing IoT cloud-based apps and cybersecurity prospects is on solving issues like those mentioned.[39]

VI. FUTURE RESEARCH DIRECTIONS

Our finding of the literature research indicates that there is a lack of experience in PaaS in most cases but IaaS and SaaS security concerns mostly are the subject of studies. Regrettably, those few studies do not even demonstrate practically or offer a method or foundation of security on which to address much of a solution. Among many other characteristics of this model, it is, obviously, either less recognizable than possible popular options, or there are lesser-known security gaps in society for this one. But now that the intelligence is currently being developed under layers, other studies will need to start exploring the security problems in this layer.

This study's other key finding is that the articles mainly concentrate on virtualization technologies' vulnerabilities. This is because the notion is central to cloud computing in a services-oriented environment. However, it is a well-researched risk, and identifying a study on each situation was very hard for the research of this paper. So virtualization is said to be categorized into four groups. Conducting comprehensive analyses of virtualization vulnerabilities was not a common occurrence in the literature. It would be advantageous to explore in the future, how security can be compromised through a single vulnerability in varied situations. These inquiry results would motivate the development of ideal practices by CSPs and users as well.

VII. CONCLUSION

Our study discusses the security issues related to service-based cloud computing by considering the highly recognized writings published in the last decade. The goal of this study is to offer a taxonomy tying vulnerabilities to corresponding countermeasures and provide a current status of the research field. To achieve this, four groups of security vulnerabilities were identified: IaaS, PaaS, SaaS, and general. The generic class has a wide range of potential vulnerabilities at all levels, but the first three classes focus on often occurring problems within the same layer. We tried to bring together the most popular security issues, which are described in the literature, although, there are many different sorts of them.

The research results showed that shared technology, session hijacking, and DoS/DDoS were the most commonly resolved problems. It was found that DDoS/DoS attacks were the most frequent issue in the cloud's medium networking security issues such as MiTC and others. However, the latter category is the domain of clouds, entailing only multitenancy. Studies show that whether the objectives, service models, or structure are the same, there are still common challenges that need more investigation later. Along with service diversity and customer preferences, cloud architectural complications may be the origin of many new security risks though. To take into account all user demands, recently the range of cloud services has become wider. Additionally, security holes are likely to be crafted for devious purposes although it offers more freedom. On the other hand, service providers and customers need to be more knowledgeable of the risks and challenges. In the literature, the majority of vulnerabilities are covered in the introduction or the traditional setup.

REFERENCES

[1] Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. Future Generation Computer Systems, 79, 849-861.

[2] Vasiljeva, T., Shaikhulina, S., & Kreslins, K. (2017). Cloud computing: Business perspectives, benefits and challenges for small and medium enterprises (case of Latvia). Procedia Engineering, 178, 443-451.

[3] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "NIST cloud computing reference architecture," in World Congress on Services, SERVICES 2011, Washington, DC, USA, July 4-9, 2011. IEEE Computer Society, 2011, pp. 594–596. [Online]. Available: https://doi.org/10.1109/SERVICES.2011.105

[4] S. Becker, G. Brataas, M. Cecowski, D. Huljenic, S. Lehrig, and I. Stupar, "Introduction," in Engineering Scalable, Elastic, and Cost-Efficient Cloud Computing Applications - The CloudScale Method, S. Becker, G. Brataas, and S. Lehrig, Eds. Springer, 2017, pp. 3–21. [Online]. Available: https://doi.org/10.1007/978-3-319-54286-7 1

[5] J. Weinman, "The economics of pay-per-use pricing," IEEE Cloud Comput., vol. 5, no. 5, p. 101, 2018. [Online]. Available: https://doi.org/10.1109/MCC.2018.053711671

[6] C. Modi, D. R. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013. [Online]. Available: https://doi.org/10.1007/s11227-012-0831-5

[7] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infrastructure-as-a-service cloud security," *ACM Comput. Surv.*, vol. 47, no. 4, pp. 68:1–68:31, 2015. [Online]. Available: https://doi.org/10.1145/2767181

[8] S. Sengupta, V. S. Kaulgud, and V. S. Sharma, "Cloud computing security trends and research directions," in *World Congress on Services, SERVICES 2011, Washington, DC, USA, July 4-9, 2011*. IEEE Computer Society, 2011, pp. 524–531. [Online]. Available: https://doi.org/10.1109/SERVICES.2011.20

[9] A. Verma and S. Kaushal, "Cloud computing security issues and challenges: A survey," in *Advances in Computing and Communications - First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV*, ser. Communications in Computer and Information Science, A. Abraham, J. L. Mauri, J. F. Buford, J. Suzuki, and S. M. Thampi, Eds., vol. 193. Springer, 2011, pp. 445–454. [Online]. Available: https://doi.org/10.1007/978-3-642-22726-4 46

[10] Manhas, S. (2022). An Interpretive Saga of SQL Injection Attacks. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 1 (pp. 3-12). Singapore: Springer Nature Singapore.

[11] J. P. Barrowclough and R. Asif, "Securing cloud hypervisors: A survey of the threats, vulnerabilities, and countermeasures," *Secur. Commun. Networks*, vol. 2018, pp. 1681908:1–1681908:20, 2018. [Online]. Available: https://doi.org/10.1155/2018/1681908

[12] IBM Cloud Education, "Iaas vs. PaaS vs. saas, understand and compare the three most popular cloud computing service models," 2021. [Online]. Available: https://www.ibm.com/cloud/learn/iaas-paas-saas

[13] A. Rashid and A. Chaturvedi, "Virtualization and its role in the cloud computing environment," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 1131–1136, 2019

[14] M. I. Malik, S. H. Wani, and A. Rashid, "Cloud computing-technologies." *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, 2018.

[15] Lozano, S., Lugo, T., & Carretero, J. (2023). A Comprehensive Survey on the Use of Hypervisors in Safety-Critical Systems. *IEEE Access*.

[16] B. Asvija, R. Eswari, and M. B. Bijoy, "Security in hardware-assisted virtualization for cloud computing - state

of the art issues and challenges," *Comput. Networks*, vol. 151, pp. 68–92, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.01.013

[17] E. Bauman, G. Ayoade, and Z. Lin, "A survey on hypervisor-based monitoring: Approaches, applications, and evolutions," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 10:1–10:33, 2015. [Online]. Available: https://doi.org/10.1145/2775111

[18] Meenakshi, S., & Neha, B. (2023). Cloud System Performance and Security Improvements with Multi-Tenancy Integration. *Journal of Multimedia Technology & Recent Advancements*, *10*(02), 10-16.

[19] E. Bauman, G. Ayoade, and Z. Lin, "A survey on hypervisor-based monitoring: Approaches, applications, and evolutions," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 10:1–10:33, 2015. [Online]. Available: https://doi.org/10.1145/2775111

[20] S. Wang, Z. Liu, Q. Sun, H. Zou, and F. Yang, "Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing," *J. Intell. Manuf.*, vol. 25, no. 2, pp. 283–291, 2014. [Online]. Available: https://doi.org/10.1007/s10845-012-0661-6

[21] Kavis, M. (2023). *Architecting the cloud*. Wiley.

[22] L. M. Vaquero, L. Rodero-Merino, and D. Moran, "Locking the sky: a survey´ on iaas cloud security," *Computing*, vol. 91, no. 1, pp. 93–118, 2011. [Online]. Available: https://doi.org/10.1007/s00607-010-0140-x

[23] A. H. Shaikh and B. Meshram, "Security issues in cloud computing," in *Intelligent Computing and Networking*. Springer, 2020, pp. 63–77.

[24] B. Cook, "Formal reasoning about the security of amazon web services," in *Computer Aided Verification - 30th International Conference, CAV 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings, Part I*, ser. Lecture Notes in Computer Science, H. Chockler and G. Weissenbacher, Eds., vol. 10981. Springer, 2018, pp. 38–47. [Online]. Available: https://doi.org/10.1007/978-3-319-96145-3 3

[25] E. N. Loukis, M. Janssen, and I. Mintchev, "Determinants of software-as-aservice benefits and impact on firm performance," *Decis. Support Syst.*, vol. 117, pp. 38–47, 2019. [Online]. Available: https://doi.org/10.1016/j.dss.2018. 12.005

[26] S. S. Manvi and G. K. Shyam, "Resource management for infrastructure as a service (iaas) in cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 41, pp. 424–440, 2014. [Online]. Available: https://doi.org/10.1016/j.jnca.2013.10.004

[27] D. Kim and M. A. Vouk, "A survey of common security vulnerabilities and corresponding countermeasures for saas," in *2014 IEEE GLOBECOM Workshops, Austin, TX, USA, December 8-12, 2014*. IEEE, 2014, pp. 59–63. [Online]. Available: https://doi.org/10.1109/GLOCOMW.2014.7063386

[28] A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. E. Ghazi, "Cloud computing: Security challenges," in *2012 Colloquium in Information Science and Technology, CIST 2012, Fez, Morocco, October 22-24, 2012*. IEEE, 2012, pp. 26–31. [Online]. Available: https://doi.org/10.1109/CIST.2012.6388058

[29] M. Almorsy, J. C. Grundy, and I. Muller, "An analysis of the cloud computing¨ security problem," *CoRR*, vol. abs/1609.01107, 2016. [Online]. Available: http://arxiv.org/abs/1609.01107

[30] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust - a security assessment model for infrastructure as a service (iaas) clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 523–536, 2017. [Online]. Available: https://doi.org/10.1109/TCC.2015.2415794

[31] Manhas, S. (2021, December). Ontology of XSS Vulnerabilities and its Detection using XENOTIX Framework. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 320-323). IEEE.

[32] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Comput. Electr. Eng.*, vol. 59, pp. 126–140, 2017. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2016.03.004

[33] A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. E. Ghazi, "Cloud computing: Security challenges," in *2012 Colloquium in Information Science and Technology, CIST 2012, Fez, Morocco, October 22-24, 2012*. IEEE, 2012, pp. 26–31. [Online]. Available: https://doi.org/10.1109/CIST.2012.6388058

[34] Bulusu, S., & Sudia, K. (2013). A study on cloud computing security challenges.

[35] Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580.

[36] Omer, M. A., Yazdeen, A. A., Malallah, H. S., & Abdulrahman, L. M. (2022). A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges. *Journal of Applied Science and Technology Trends*, *3*(02), 101-111.

[37] David, D. S., Anam, M., Kaliappan, C., Selvi, S., Sharma, D. K., Dadheech, P., & Sengan, S. (2022). Cloud Security Service for Identifying Unauthorized User Behaviour. *Computers, Materials & Continua*, *70*(2).

[38] Lozano, S., Lugo, T., & Carretero, J. (2023). A Comprehensive Survey on the Use of Hypervisors in Safety-Critical Systems. *IEEE Access*.

[39] Manhas, S., & Taterh, S. (2018). A Comparative Analysis of Various Vulnerabilities Occur in Google Chrome. In Soft Computing: Theories and Applications: Proceedings of SoCTA 2016, Volume 1 (pp. 51-59). Springer Singapore.

[40] K. Kritikos, T. Kirkham, B. Kryza, and P. Massonet, "Towards a security-enhanced paas platform for multi-cloud applications," *Future Gener. Comput. Syst.*, vol. 67, pp. 206–226, 2017. [Online]. Available: https://doi.org/10.1016/j.future.2016.10.008

[41] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, "Cloud computing security issues in infrastructure as a service," *International journal of advanced research in computer science and software engineering*, vol. 2, no. 1, 2012.

[42] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2016, pp. 117–123.

[43] E. B. Chawki, A. Ahmed, and T. Zakariae, "Iaas cloud model security issues on behalf cloud provider and user security behaviors," in *The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks andCommunications (FNC-2018) / Affiliated Workshops, Gran Canaria, Spain, August 13-15, 2018*, ser. Procedia Computer Science, A. Yasar and E. M. Shakshuki, Eds., vol. 134. Elsevier, 2018, pp. 328–333. [Online]. Available: https://doi.org/10.1016/j.procs.2018.07.180

[44] N. Khan and A. Al-Yasiri, "Identifying cloud security threats to strengthen cloud computing adoption framework," in *The 11th International Conference on Future Networks andCommunications (FNC 2016) / The 13th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2016) / Affiliated Workshops, August 15-18, 2016, Montreal, Quebec, Canada*, ser.Procedia Computer science,E.M.Shakshuki,ed,vol.94.Elsevior,2016, pp. 485–490.

[45] Manhas, S., Taterh, S., & Singh, D. (2020). Deep Q learning-based mitigation of man in the middle attack over secure sockets layer websites. Modern Physics Letters B, 34(32), 2050366.

[46] M. T. Sandikkaya and A. E. Harmanci, "Security problems of platform-as-a service (paas) clouds and practical solutions to the problems," in *IEEE 31st Symposium on Reliable Distributed Systems, SRDS 2012, Irvine, CA, USA,*

October 8-11, 2012. IEEE Computer Society, 2012, pp. 463–468. [Online]. Available: https://doi.org/10.1109/SRDS.2012.84

[47] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint: Iaas, paas and saas," in *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems, Caraguatatuba, Brazil, October 25 - 29, 2015*, R. Chbeir, Y. Manolopoulos, V. P. Mammana, E. A. Modena, A. J. M. Traina, O. S. S. Filho, Y. Badr, and F. Andres, Eds.` ACM, 2015, pp.148–155. [Online].Available:https://doi.org/10.1145/2857218.2857253

[48] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2016, pp. 117–123.

[49] Manhas, S., Taterh, S., & Singh, D. (2019). A Novel Approachfor Phishing Websites Detection using Decision Tree.

[50] K. McKay and D. Cooper, "Guidelines for the selection, configuration, and use of transport layer security (tls) implementations (2nd draft)," National Institute of Standards and Technology, Tech. Rep., 2018.

[51] G. Verma and S. Adhikari, "Cloud computing security issues: a stakeholder's perspective," *SN Computer Science*, vol. 1, no. 6, pp. 1–8, 2020.

[52] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing¨ vulnerabilities," *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 50–57, 2011. [Online]. Available: https://doi.org/10.1109/MSP.2010.115

[53] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: Solutions and future directions," *J. Comput. Sci. Eng.*, vol. 9, no. 3, 2015. [Online]. Available: https://doi.org/10.5626/JCSE.2015.9.3.119

[54] M. A. Khan, "A survey of security issues for cloud computing," *J. Netw. Comput. Appl.*, vol. 71, pp. 11–29, 2016.[Online].Available:https://doi.org/10.1016/j.jnca.2016.05.010

[55] K. Selvamani and S. Jayanthi, "A review on cloud data security and its mitigation techniques," *Procedia Computer Science*, vol. 48, pp. 347–352, 2015.