A Review on Cloud Computing Threats, Security and Possible Solutions

Hafiz Muhammad Faisal Shehzad[1], Rabia Naz[2], Asia Muneer[1], Abid Rafiq[1], Samreen Razzaq[1], Mudassar Ali Shah Zaidi[1]
[1]Department of CS and IT, University of Sargodha, Sargodha, Pakistan
[2]Department of SE, University of Sargodha, Sargodha, Pakistan
*Correspondence. Rabia Naz; rabianaz935@gmail.com

Citation | Shehzad. H. M. F, Naz. R, Muneer. A, Rafiq. A, Razzaq. S, Zaidi. M. A. S, "A Review on Cloud Computing Threats, Security, and Possible Solutions", IJIST, Vol. 6 Issue. 3 pp 1417-1437, Sep 2024
Received| Aug 12, 2024, **Revised|** Sep 8, 2024, **Accepted|** Sep 14, 2024, **Published|** Sep 16, 2024.

Cloud computing is increasingly popular, with major companies like Microsoft, Google, and Amazon creating expansive cloud environments to support vast user bases. Despite its benefits, security remains a significant concern, complicating full trust in cloud solutions due to potential hazards and the consequences of security breaches. This study introduces a novel approach to address the gaps in existing frameworks for summarizing and analyzing cloud security issues and requirements. We explored various cloud computing security challenges, assessed the impact of different cloud models, and discussed risk mitigation techniques and policies for both cloud providers and users. Our analysis offers a comprehensive examination of security risks affecting cloud computing, alongside the latest security solutions. Rather than focusing solely on specific issues, we presented a broader perspective on advanced, high-level security frameworks. We outlined multiple strategies for developing a secure, reliable, and cost-effective cloud infrastructure.

Keywords. Vulnerabilities of Cloud Computing; Security Threats; Data Security; Cloud Computing.

Introduction.

In today's multi-distributed cloud environments, cybersecurity concerns have grown increasingly complex, impacting various aspects of the client-server architecture. The European Network and Information Security Agency has identified potential threats and proposed solutions for cloud computing systems. Shamshirband et al. [1] have concentrated on managing intercommunication activities to enhance security. Common vulnerabilities in cloud networks include ARP spoofing, DoS/DDoS attacks, DNS flaws, and IP spoofing [1]. Additionally, Advanced Persistent Threat (APT) attacks have surged by 70%, with suspicious activities increasing by 68% and brute force attacks rising by 56% [2]. APT attacks involve unauthorized network access and prolonged covert operations. Recent developments reveal new security concerns. Specifically, attacks on cloud services are growing at an alarming rate, where ransomware attacks have risen by 90% over the past two years and AI-based attacks have gone up by 60%. These trends pose a significant weakness in the existing security models.

The International Data Center (IDC) conducts a study of cloud computing issues and collects data and opinions from leaders every year and up to 87% of the clients mention security and privacy as their top priority [3]. Nevertheless, there has been extensive literature on the aspect, but most of it has been dedicated to advancing cloud security models rather than other important research areas. This underscores the need for continued assessments of security risks to make adequate security measures to safeguard clouds as a service.

This study seeks to fill this gap by proposing a novel security framework that incorporates AI systems and homomorphic encryption for threat identification. This view is supported by the study, which shows that despite employing several security measures, human error remains a factor and no system is impervious to intrusion. The goal of the proposed work is to offer a comprehensive analysis of critical security issues with the help of such viewpoints as public and private clouds. The study, in particular, outlines security standards for management and IT, encryption plans, disasters, and the backup procedure. It outlines viable strategies for protecting cloud infrastructure and identifies other unsolved problems. Moreover, the studies evaluate the existing cloud security level and provide a depiction of the existing state to improve the comprehension of the preeminent concepts. This study aims to resolve outstanding security concerns and enhance cloud security, for which purpose the researcher examines prior works and assesses attempts worldwide to progress cloud computing.

Literature Review.

Cloud computing security has been extensively researched. Ahmad et al. [3] advocate for thorough security assessments that encompass risks, vulnerabilities, and classifications. Their study [4] examines organizational, legal, architectural, and communication issues, focusing on vulnerabilities related to virtual machine migration, hypervisors, and VM images, and proposes countermeasures for message inquiries. Based on this, more detailed information on how to construct safe cloud structures is given by Bharany et al. [5]. The researchers explained how to strengthen the cloud structures against possible risks by concentrating on the architectural and functional elements of security solutions. This view is useful in building a secure cloud context but could be insufficient to address the constantly evolving threats.

Regarding the safety of cloud computing, Tabrizchi et al. [6] present potential solutions in service modeling simulations. The authors of the research propose techniques to reproduce and evaluate approaches of cloud services concerning threats of safety breaches, and hence offer means for the early detection of threats. However, it may not be very effective in actual operations, since the simulations do not always portray the whole operational environment and risks. In the area of privacy, trust, and secrecy, Valluripally et al. [7] identified and discussed major issues/concerns and solutions for enabling dependable cloud computing. Another recent study [8] extends the discussion by providing a comprehensive framework of a multilayered cloud environment that interconnects cloud, computing with the IoT. This research addresses

data mining and vehicular cloud services and aims to propose a new software architecture for vehicle data clouds. This paper contributes to the literature on cloud computing with IoT yet it may fail to explain the basic tenets of security in cloud computing across different environments.

Parast et al. [9] presented a detailed account of privacy and security issues and revealed various explanations, as well as proposed further research avenues. Analyzing current issues is useful but does not present a singular methodology that can tackle the complexities of cloud security. Gaurav et al. [10] presented a general outline of threats and opportunities in cloud computing, as well as solutions to them in today's world. While the review is useful in offering an all-around view of the area, it can be brief on the details of the vulnerabilities or proposed countermeasures. Nguyen et al. [11] used a similar approach where they systematically explored cloud security issues based on the traits of clouds.

This review indicates a significant need for a unified framework that integrates various security elements discussed in the literature. The current study addresses this gap by proposing a comprehensive framework designed to enhance cloud security across multiple dimensions. The proposed threat model aims to achieve an effective, private, secure, trustworthy, and cost-effective cloud system, as illustrated in Figure 1. By consolidating insights from the diverse approaches and addressing the limitations identified in previous research, this study seeks to provide a holistic solution to the challenges faced in cloud computing security.

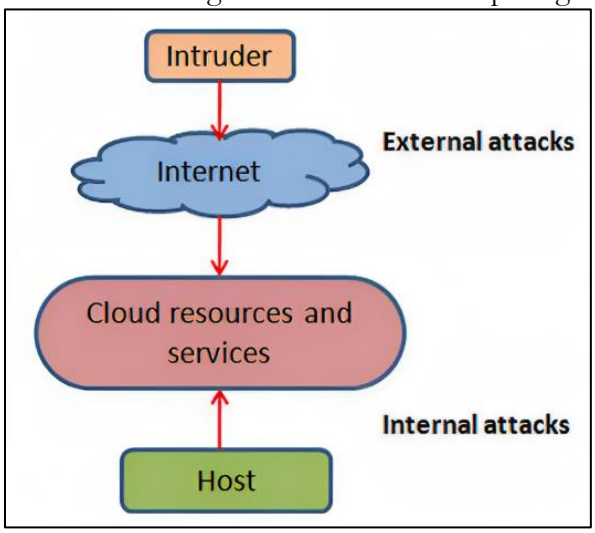

Figure 1. Threat Model in Cloud Computing

Materials and Methods.

This section explores the security dimensions, distinct security zones, threats, and challenges associated with cloud computing. It outlines strategies implemented to ensure secure cloud environments and addresses how these issues are managed.

Security Dimensions.

This subsection is a brief overview of what cloud computing security comprises, including software security, infrastructure security, and capacity security.

- **Software Security.** It is essential to guarantee that software will run smoothly and continuously under constant aggravation by viruses. In a cloud computing environment especially where SaaS dominates, secure software is mandatory. The attacks involving software security can cause problems with implementation and buffer overflow.
- **Infrastructure Security**. Cloud providers are under pressure to prove the accuracy of both the logical and physical systems. Simply relying on third-party verification is not enough for business owners or data managers. Manufacturers demand proof that the cloud infrastructure is capable of supporting basic business activities with a high degree of capability and reliability.

- **Capacity Security.** In cloud computing, a user uploads or inputs their information into the cloud rather than managing it. This aspect of cloud data storage is therefore important in delivering quality services. Encryption of data, checking the actual deletion of data that has been distributed, permanency or archival of data, confidentiality, and privacy both in communication and storage, and malware control.

Distinctive Zones of Security Issues.

This section discusses various security threats to embedded systems and concentrates on some of the features like virtual machine isolation, programmability, electronic access control, and the like. It identifies the strategic activities and management of risks in each zone with the corresponding measures and/or strategies.

- **Virtual Machine Isolation.** One of the key considerations in cloud architecture is to achieve substantial isolation between Virtual Machines (VMs). The failure to attain such goals exposes systems to cross-VM attacks and leads to data breaches [5]. Subsequent advancements and enhancements made to VM isolation have been aimed at enhancing the security of cloud environments. Some of them include micro-segmentation and hardware-based isolation. Micro-segmentation splits the network into the smallest and completely isolated portions to limit the consequences of the breach to a segment. There are platforms like Intel SGX (Software Guard Extensions) that provide the provision of securing specific parts of an application even from OS.
- **Programmability.** Programmability plays a key role in cloud computing, impacting functionalities such as accounting, anomaly detection, and more. Programmable processor packages at each port support these functions. One challenge is implementing packet inspection features for software development, as many network processing environments rely on low-level abstractions to achieve optimal throughput [12].
- **Electronic Access Control System.** The Electronic Access Control System (EACS) is crucial for managing authentication and edge security when transmitting client data across the cloud network. The Security Assertion Markup Language (SAML), a federated protocol including authentication credentials, facilitates this process. Simple Object Access Protocol (SOAP) is an XML-based protocol used for request and response structures in SAML. Despite digital signatures, a signature-wrapping attack could potentially alter a message, allowing a hacker to impersonate a legitimate user [13].
- **SNMP Server.** The Simple Network Management Protocol (SNMP) Server collects data from network devices efficiently. However, due to its development by individuals with diverse programming backgrounds, it may be susceptible to security vulnerabilities.
- **User Frontend.** The security of the user interface should be organized in layers, similar to an onion. However, improper configuration and unauthorized access remain significant risks. Developers need to have an understanding of the security risks associated with web development languages including; HTML, CSS, PHP, and JavaScript. For example, Tabrizchi et al. [6] have demonstrated that breaches or code injection affect isolation barriers, therefore the importance of having a strong front end in case the attacker has already gained access to the back end via the database.
- **Framework.** IBM splits security into five categories in their stylization of the model. Audit and compliance, access, flow, identity, and configuration [14]. Developed in Java and NET, this framework provides adequate ways for monitoring and protection of the resources despite some difficulties such as the problems that arise from the termination of threads.
- **Application Licensing.** Concerning the issue of the key challenge to the conversion of applications to cloud service, licensing of applications is still a center of concern. Other illegitimate software usage like copying, selling, sharing, or distributing software poses a major security threat. Having more unlicensed software consequently enhances the risks of security as

many servers hosting various applications are expected to remain online, be scalable, and be reliable [15].

- **Service Availability.** When it comes to developing the service availability on the cloud there several important factors to consider that fall under the SaaS PaaS and in some cases IaaS categories. To achieve the objectives of elasticity and high availability each service type has to guarantee that applications and infrastructure are equipped to handle changes in the cloud environment [16].
- **Parallel Programs.** Parallel programs increase the capabilities of a system adding some complexities when executing the programs. This is because authentication issues come up when several programs are concurrently running and thus make it an area of concern in terms of vulnerabilities. Additionally, severe load imbalances caused by non-uniform data distribution can affect the performance of parallel algorithms [17].

Web Application Security.

Distributed computing significantly influences various technologies such as Web 2.0, virtualization, and service-oriented architecture (SOA), as noted by Ahmad et al. [4]. This integration, however, also brings to light several security vulnerabilities. These vulnerabilities, inherent to distributed architectures, can jeopardize the integrity of Software-as-a-Service (SaaS) applications. Potential threats include man-in-the-middle attacks, port scanning, IP spoofing, social engineering, and injection holes, which can lead to unauthorized actions if attackers compromise slave PCs. Elmasry et al. [18] emphasized a critical aspect of web technology, data integrity, examples of compromised data integrity include.

- **Equifax Data Breach (2017).** A data breach that led to the exposure of the personal identification information of 147 million people. In their case, the breach was caused by hackers exploiting an unpatched software vulnerability.
- **Capital One Data Breach (2019).** Caused by unauthorized access to credit card data as a result of misconfigured web application firewalls.

Compromises in web servers, especially in cloud-based environments, can result from activities such as altered XML data injection, illegal surveillance, or breached server authentication. As internet connectivity expands through various devices, including chat servers, attackers increasingly exploit these vulnerabilities. A common risk is direct object reference, where internal objects like private files or database entries become accessible to unauthorized users. Attackers who manipulate these references can exploit server-side scripting to gain unauthorized access to the operating system and database [19]. Proxy server security is another area of concern. Denial of Service (DoS) attacks often utilize compromised systems as proxies to mask the attacker's identity. Attackers leverage open proxies to gain unauthorized access to multiple websites while obscuring their connections. This practice introduces several security risks, such as obfuscation, 400 errors, RPAs, and X-Forward-For header manipulations [20].

Trust and Conviction.

Trust in cloud services is often grounded in confidence from past experiences, influencing decision-making reliability. Shi et al. [21] advanced security transparency within the TCP framework to ensure data confidentiality and integrity. Trust assessment is complex, involving multiple dimensions.

- **Human Factor**. Human behavior plays a significant role in both creating and mitigating security risks. Unpredictable human actions make it challenging to implement flawless security measures. The behavior of IT and non-IT personnel can significantly impact system security. Issues such as managing passwords across multiple nodes and social engineering attacks (e.g., phishing, baiting) underscore the importance of human factors in cloud security [22].
- **Digital Forensics Significance**. The rise of digital crimes necessitates robust digital forensics. Key areas include data capture, localization, disclosure, and compromise. The Bring

Your Device (BYOD) trend introduces additional challenges for digital forensics [23][24]. Some challenges that BYOD is bringing have been addressed by digital forensics with several tools. Mobile Device Management (MDM) ensures that employees' devices use secure mechanisms when accessing company resources. These devices are alike monitored by Endpoint Detection and Response (EDR) even when they are off the corporate network for any signs of a compromise. Similar to security, blockchain technology is also been applied in forensics for the conformity purpose of ensuring that evidence remains intact and unaltered, especially when devices are decentralized like in the case of BYOD.

- **Reputation Management**. The growth of cloud computing has heightened interest in reputation management. In a cloud environment, virtual machines share hardware, creating reputation dependency. Malicious activities by some users can affect the entire cloud ecosystem, leading to potential legal consequences during investigations [25].
- **Challenges in Managing Cloud Environments**. Migrating to cloud environments presents significant governance challenges, particularly in Infrastructure as a Service (IaaS) contexts. Issues include understanding financial implications, recovery, disaster planning, liability for data breaches, service termination, and potential business closure [3].
- **Role of Trusted Third Parties (TTPs)**. TTPs are crucial for validating and protecting sensitive data. They provide a layer of defense against breaches but pose a risk if compromised. Luo et al. [26] proposed using private key systems and data shading techniques to create a trustworthy network across multiple data centers.
- **Consumer Trust Challenges**. Research indicates low trust in online service providers, with only 33% of Europeans trusting phone and internet service providers and 22% trusting search engines and social media platforms. Concerns about personal data security are widespread and influenced by factors such as reputation, reliance on TTPs, previous experiences, and organizational aspects [19].

Customer Administration Issues.

This section explores security challenges in customer management within cloud computing, including client experience, authentication, privacy, and service level management.

- **Cloud Computing Administration**. Customer management presents a major security challenge, akin to protecting a high-profile individual in different contexts. The security risks associated with public cloud data differ from those of data within organizational systems [27].
- **Client Experience (CX)**. Ensuring a positive client experience in cloud services is crucial. Some providers face difficulties due to a lack of clear cloud-based solutions, which can complicate secure service selection for users with limited security expertise.
- **Customer Authentication**. Effective authentication is essential for securing cloud services. Pieroni et al. [28] analyzed various authentication threats, including eavesdropping, password leakage, token interception, cookie tampering, and man-in-the-middle attacks. Providers must ensure that only authorized users gain access across multiple devices and locations.
- **Customer-Driven Privacy**. Businesses are increasingly focusing on customer-centric cloud services. A 2015 survey of IT executives revealed a shift toward prioritizing service requirements, security, privacy, trust, and CRM strategies [21].
- **Service Level Management**. Service level management involves setting standards, tracking performance, and ensuring adherence to client expectations. Issues such as poorly installed security systems and inadequate response to critical vendor alarms can challenge the effectiveness of security safeguards within service-level agreements [29].

Security Challenges.

This section addresses various security challenges in cloud computing, including data tampering, DoS/DDoS attacks, data emission, unauthorized access, and weak configuration standards.

- **Data Alteration**. Man-in-the-middle attacks aim to modify data packets by altering flow rules, impacting the data plane, control plane, and southbound interface.
- **DoS/DDoS Attacks**. Attackers can flood controller-switch communications, leading to switch flow table saturation and Denial of Service. DDoS attacks involve multiple bots generating fraudulent traffic that mimics real traffic, overwhelming resources and causing service disruptions [30].
- **Data Emanation**. Side channel attacks on input buffers can expose credential management information, such as keys and certificates, leading to vulnerabilities in the control plane and data plane.
- **Unauthorized Access**. Resources across various cloud layers are at risk if attackers gain authentication. Unauthorized applications can breach security in the northbound interface and control plane.
- **Weak Configuration Policies**. Inadequate TLS adoption and weak policy enforcement can undermine the entire cloud architecture, affecting the application plane, controller, and northbound interfaces [31].

Figure 2 shows the summarized view of security challenges in the cloud computing.

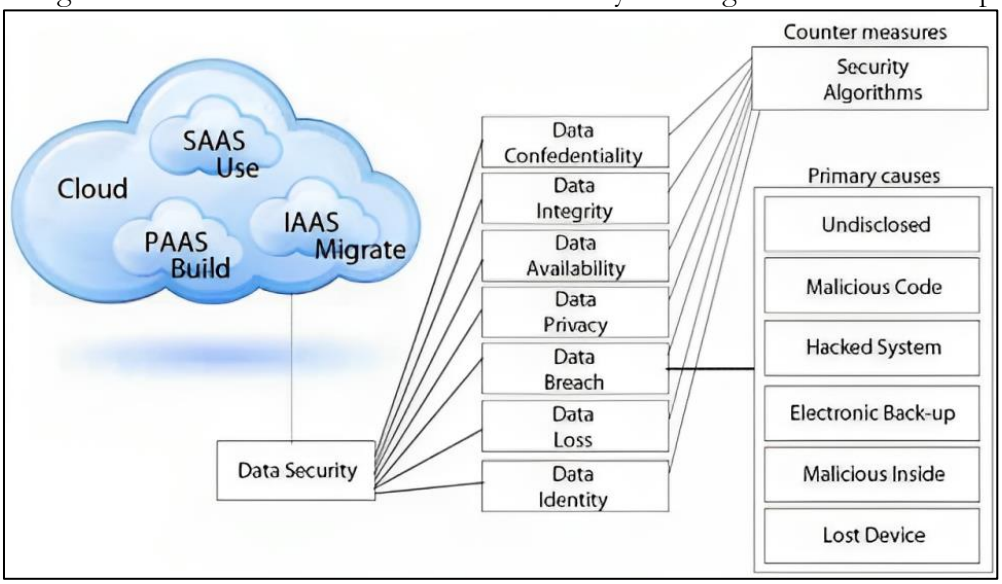

Figure 2. Security Challenges in Cloud Computing

Security Attacks.

This section classifies and examines various types of security attacks targeting cloud computing environments, detailing the techniques and consequences of each attack type.

Data Plane Attacks.

- **Denial of Service (DoS)**. With DoS attacks, the attacker utilizes an already infected host to flood the network resources and halt the services offered.
- **Man-in-the-Middle (MitM) Attack**. MitM is a type of network attack where the attacker situates himself between the sender and the receiver and can intercept or modify the data sent between the two parties.
- **Malicious Traffic Injection**. Attackers insert harmful flow rules into network devices using protocols like OpenFlow (OF), Open vSwitch Database Management Protocol, or PCEP, compromising network integrity.
- **Relay Attack**. By intercepting and replaying communication, attackers conduct relay attacks through techniques like flow eavesdropping [32].

- **DoS Attack at Data Center Interconnect (DCI) Connections**. This attack involves injecting high volumes of false traffic into the DCI cables and stations; due to poor DCI protocol architectures and poor data packet encryption, this lowers the security of data centers.

Control Plane Attacks.

- **Vulnerable Security Configurations**. Many controllers are not set up with correct security settings and no adequate passwords. Most are installed with default configurations on operating systems such as the Linux OS and can be run with controllers with certain bugs.
- **Rogue Controller Implementation**. Attackers deploy rogue controllers to manipulate flow tables undetected, giving them unauthorized control over the network. A lack of trust between controllers and management applications can lead to data breaches. The security community notes that TLS/SSL may not provide adequate protection, as it relies on trust between controllers and network devices (e.g., routers, OpenFlow switches) and the PKI infrastructure [20].
- **Resource Consumption Attacks**. Attackers deplete the controller's resources, causing delays in responding to events like PacketIn and PacketOut messages. This reduces the controller's efficiency and overall network performance.
- 3.7.3. General Attacks
- **Know Your Enemy (KYE) Attacks**. These attacks aim to gather sensitive information and intelligence on policy enforcement methods. KYE attacks are successful when attackers install malicious policies on switches, allowing them to disable intrusion detection/prevention systems.

Testing Methodology.

To prove the viability of the proposed framework in mitigating the threats related to cloud computing and achieving security, several strategies will be used. This includes simulations, case studies, and the application of theories in real-life scenarios. Specific scenarios of cloud security will be tested in simulations, such as stress tests in the framework of DoS and DDoS attacks, as well as MitM attacks. These simulations will utilize data emulation to model a regular cloud data flow and assess the effectiveness of this framework in terms of data manipulation and leakage protection.

Real-life examples of such scenarios will be incorporated into case studies to assess the applicability of the framework in practice. This comprised applying the framework in environments integrated into cloud providers, where the outcomes regarding the handling of virtual machine isolation, electronic access control, and the programmability of such environments were to be assessed. Case studies will also include assessing the framework performance in addressing threats like buffer overflow vulnerabilities and cross-VM attacks.

The evaluation criteria will be applied to real scenarios that will involve live cloud setup. They will be implemented in pre-existing cloud solutions architecture and deployed with the primary aim of evaluating the effects of the framework on software security, capacity security, and security of the infrastructure. This practical implementation will assist in evaluating the impact of the framework at the practical level toward solving such questions as data encryption, data deletion checks, and protection from virus programs.

Furthermore, emerging solutions including artificial intelligence (AI) threat hunting and homomorphic encryption will also be integrated into the framework. Self-learning threat hunting with the use of AI will help actively and continuously identify threats and threats from activities conducted within a cloud environment based on the pattern and behavior found. Private Information Retrieval will be overviewed to allow for data analysis and processing using the services of a cloud without losing its privacy and revealing it to the cloud.

Results.

This section discusses various solutions, strategies, and challenges for protecting cloud computing systems, focusing on protection techniques, architecture design, software-defined security, data storage, and service security.

Protection of Cloud Computing.

- **Robust Flow Control**. Zhang et al. [33] propose the OpenFlow Random Host Mutation technique to protect IP addresses against attackers. Alam et al. [34] propose random route mutation to improve security against DDoS and DoS threats. While it appears to be an effective solution in diversifying the traffic routes, its adaptation to large-scale settings involves extensive modification in the existing physical network requirements that are both expensive and time-consuming.
- **Global Visibility**. Centralized network control is made feasible by the broad reach of cloud computing and therefore can provide for monitoring of activity, data collection, and response to threats. This increased visibility is useful in the detection and prevention of potential security threats. For instance, control systems such as those applied at Amazon Web Services (AWS) use global visibility to identify threats and prevent them in many zones. But it is accompanied by some risks, for example, LOVs, SPOFs, and highly skilled personnel are needed to operate complex monitoring tools.
- **Advanced Data Plane Security**. It comprises AvantGuard and OFX (Open Financial Exchange). AvantGuard is an electronic security system that involves, monitoring security systems as well as giving timely notifications and reactions. These are the self-diagnostic mechanisms where the system itself can hypothesize and trigger alarms to authorities or users in cases of anomalies. It provides a simple and scalable approach for the protection of the data plane. OFX is a working protocol used to facilitate secure and standard transactions of financial data between organizations, which is critical for cloud-based financial applications. It improves the security of OpenFlow switches, and OpenSDWN expands the capabilities of wireless access points with virtual middle-boxes. These enhanced security measures cost a lot of resources, or such issues as compatibility with older systems or expansion of the solution to worldwide cloud networks may prove to be an issue.

Secure Cloud Computing Architecture Design.

- **Secure Controller**. Controllers' calls must be protected against unauthorized access and should have more layers of security before reaching the master controller's access. In practice, the approach of using multiple layers of security could introduce performance issues such as bottlenecks and the integration of controller access in large-scale cloud systems may become difficult.
- **Global Availability**. Cloud computing controllers should have secure and effective measures of control and be on standby to ensure continuous network operations are happening. Maintaining global availability is not always easy because the system may be vulnerable to risks such as hardware breakdown, power failure, and DDoS attacks. Backup systems have to be put in place and there are always backup systems which are often expensive to sustain.
- **Performance Monitoring Framework**. The architecture should be adaptable for supervising and modifying the performance of the controller for its intended use. Supervising performance in real-time can be difficult, primarily across multiple systems in a distributed environment because of delays in data transfer and the sheer volume of data received, which means that performance degradation can go unnoticed for some time.
- **Anomaly Detection and Remediation**. Systems should be able to detect any behaviors that are out of the ordinary and that might signify a security threat [31]. While it is possible to use anomaly detection systems that are a critical component in a system the use of such systems leads to the creation of alerts which are in many cases false and causes undue attention thus

spending a lot of time managing them in case of a real attack. The process of fine-tuning these systems so that fewer 'false alerts' are given is important but can be a long and challenging process.

Software-Defined Cloud Security (SDCSec) Design.

- **Controller Redesign**. Develop controllers that meet the highest level of security through empirical research and evaluation. To improve the security levels, redesigning the controllers may lead to increased system complexity, therefore, considerable numbers of personnel to be retrained, and also existing systems may need to be reconfigured.
- **Controller Improvement**. Guard the controllers in two steps, 1) defending the controllers against external influences, and 2) minimizing communication to only essential processes. Despite such enhancements in security that are accorded by this approach, the degree of flexibility usually accorded the controller could be lacking and the controller might be unable to interact with other crucial cloud services effectively thus dragging down system performance.
- **Consistent Controller Updates**. Update controllers periodically and check the memory usage, interface statistics, and number of CPU accesses. However, updating must be done as often as possible, which may result in system instability and or system downtime. Cloud providers have to constantly update their services while, at the same time, ensuring that they remain available to clients.
- **Record Analysis**. Records should be reviewed to be able to check whether the thresholds and alarms for the centralized controllers have been set correctly [35]. The problem is to set proper thresholds to distinguish normal and abnormal activities across the different cloud infrastructures, which might take much time to achieve.

The Solution for Unauthorized Access.

Unauthorized access by unapproved hosts must be effectively prevented in cloud computing environments. The following solutions address this issue.

- **AuthFlow**. AuthFlow enhances security by employing host credential-checking techniques. Pliatsios et al. [36] introduced OpenFlow control layers that implement role-based permissions, bridging security gaps between controllers, data plane communication, and OpenFlow applications. To further secure cloud computing, a hierarchical system of switches or controllers can be utilized, minimizing the risk of failures [37]. This system, coupled with signature algorithms, ensures distributed control security by managing and installing flow rules. However, the complexity of hierarchical systems may introduce latency and coordination challenges between different control layers, particularly in large-scale deployments.
- **Self-Organizing Maps (SOMs)**. SOMs help detect and mitigate DoS and DDoS attacks by monitoring traffic patterns on OpenFlow switches. They face challenges such as high false-positive rates, requiring sophisticated tuning. Contemporary methods, like unsupervised deep learning models (e.g., autoencoders) and reinforcement learning (e.g., Deep Q-Networks), offer improved adaptability. Unsupervised models detect anomalies by learning from data without labeled examples, while reinforcement learning dynamically optimizes defense strategies in real time. These approaches can better handle evolving threats but may require significant computational resources and extensive training data.
- **DDoS Block Applications (DBA)**. DBAs monitor flow metrics at the controller level and can retransmit fraudulent traffic with a new IP address, preventing compromised hosts (bots) from operating effectively. While effective, DBA solutions may require high computational resources and could be challenging to scale across global cloud infrastructures. Additionally, legitimate traffic might be mistakenly flagged as fraudulent, causing service disruptions. AI-based prediction models can enhance DDoS protection by analyzing historical traffic patterns to anticipate attacks before they fully occur. These models use machine learning to detect anomalies and adjust defenses proactively, reducing the likelihood of false positives

and improving response times. However, they require significant computational resources and continuous tuning to stay effective against evolving threats.

- **DDoS Defender**. This advanced tool utilizes OpenFlow and Locator protocols to differentiate between legitimate and unauthorized sources. Each host has a fixed identity and a dynamic locator that changes with each movement. Network analysts use cloud computing techniques at the controller to detect traffic volume. If the volume exceeds a set threshold, the controller identifies and drops suspicious packets. Despite its robustness, DDoS Defender might face difficulties in environments with high mobility or dynamic IP allocation, where frequent locator changes could complicate the identification process and lead to delays in mitigating attacks.

Cloud Data Storage.

Data storage is a critical component of cloud computing, driven by the increasing use of web applications and internet-enabled devices.

- **Data Storage Facilities**. Data warehouses (DWHs) support various user networks with unique security needs. Ensuring the security of stored data is crucial for maintaining Quality of Service (QoS) [38]. Recent studies highlight secure multi-cloud strategies, which distribute data across multiple providers to enhance resilience and reduce risks. Additionally, blockchain technology is used to ensure data integrity and auditability by providing a tamper-proof ledger and real-time audit trails. Scalability of security measures remains a challenge as data volume grows, requiring effective balancing of resources to maintain QoS.
- **Anonymity**. Anonymity involves techniques and protocols that obscure the identity of data owners while protecting shared data. In cloud environments, insufficient security measures can lead to de-anonymization attacks [39]. Modern techniques to enhance anonymity include differential privacy, which adds noise to data; homomorphic encryption, which allows computations on encrypted data; and secure multi-party computation (SMPC), which ensures confidentiality during joint data processing. However, these methods can complicate data retrieval and auditing, impacting accountability and forensic investigations.
- **Ensuring Access**. Cloud services aim to guarantee seamless access to software, data, and hardware infrastructure from any location. However, multi-tier architectures, which utilize load balancing across multiple servers, are vulnerable to network-based attacks and service disruptions [40]. Availability issues may arise due to network flooding or malicious insider actions. Implementing redundant and geographically distributed backup systems is essential to mitigate these risks but may increase operational costs and complexity.
- **Data Security Issues**. Intrusions can cause data breaches, and hard disk failures without backups can lead to data loss. Such incidents undermine privacy, confidence, and Service Level Agreements (SLAs), which are critical for cloud users. Data leakage, particularly in web applications, is common due to improper permissions in cloud deployments [41]. To counter these issues, cloud providers need to implement regular security audits and enforce strict access control policies. However, these measures can be resource-intensive and may require constant updating to adapt to evolving threats.
- **Cryptography Challenges**. Ineffective security measures can compromise cryptographic tools. Issues include poor key management, inefficient algorithms, and data safety concerns [42]. Key management remains a particularly challenging area, as it requires secure storage and distribution of keys across potentially global networks. Mishandling can lead to unauthorized access or data corruption.
- **Integrity and Confidentiality**. Maintaining the CIA triad (Confidentiality, Integrity, and Availability) is fundamental in cloud storage. Ensuring data integrity involves maintaining accuracy and reliability while protecting confidentiality involves safeguarding sensitive data from unauthorized access and manipulation [43]. Privacy can be threatened by deceptive techniques,

stolen credentials, covert data interception, and manipulative human interactions. Cloud providers must continuously update their encryption and access control mechanisms to counteract these threats, but the dynamic nature of cloud environments makes this an ongoing challenge.

Threats in Cloud Computing.

Cloud computing faces various threats that can impact its operation.

- **Inappropriate Governance**. Centralized management in public clouds can pose security risks. Cloud service agreements often lack specific details and liabilities, leaving security gaps. For instance, the lack of standardized security protocols across different cloud providers can lead to vulnerabilities, especially in hybrid cloud environments. Organizations must negotiate clear SLAs and ensure that providers adhere to established security standards.
- **Ambiguity in Responsibility**. Cloud computing splits security responsibilities between the provider and the user. This division of responsibility can create vulnerabilities, with different services (SaaS, IaaS, PaaS) assigning varying levels of responsibility. Clear delineation of security responsibilities is crucial. Providers and users must establish comprehensive security frameworks and regularly review and update their responsibilities to mitigate risks.
- **Authentication and Authorization**. The global accessibility of cloud services raises concerns about authentication and authorization security. Effective methods are needed to establish robust authentication and authorization protocols for secure access. Implementing multi-factor authentication (MFA) and advanced authorization techniques can significantly enhance security, but these measures can also introduce complexity and user friction. Balancing security with usability is an ongoing challenge.

Services Security.

The evolving cloud computing domain integrates SaaS, Web 2.0 technologies, and utility computing to leverage the Internet while fulfilling customers' service needs. SaaS, as the dominant cloud service model, demands heightened security measures. Analysts and security consultants have identified seven key security vulnerabilities that cloud computing vendors must address.

- **Privileged User Access**. Effective management mechanisms are needed for handling user information, requests, and privileged access to cloud policies. Managing privileged access is critical to preventing insider threats and unauthorized access. Implementing role-based access controls (RBAC) and regularly auditing privileged accounts can help, but these measures can be complex to administer and require continuous monitoring.
- **Regulatory Compliance**. Vendors must provide transparency regarding their external audits and security certifications. Ensuring compliance with various regulatory requirements, such as GDPR or HIPAA, can be challenging due to the evolving nature of regulations and the need for ongoing compliance checks and documentation.
- **Data Location**. The physical location of user data must be managed by the vendor, with clear policies in place regarding data sovereignty and jurisdiction. Vendors must navigate varying national regulations regarding data location and sovereignty, which can complicate data management and compliance efforts.
- **Information Isolation**. Encryption strategies must be rigorously tested and implemented by qualified professionals. Encryption should be applied at all levels to ensure data protection. Testing encryption implementations thoroughly is necessary to prevent vulnerabilities, but this can be resource-intensive and may require specialized expertise.
- **Recovery**. Vendors should have a clear plan for data recovery and handling in the event of system failures. Data recovery plans must be regularly tested to ensure effectiveness, which can be complex and costly, particularly in large-scale or multi-cloud environments.

- **Investigative Assistance**. Vendors must have the capability to investigate and address any improper or illegal activities. Providing effective investigative assistance requires sophisticated tools and skilled personnel, which can be challenging to maintain and may incur additional costs.
- **Long-Term Feasibility**. Policies should address the handling and return of information if the vendor ceases operations, ensuring data retrieval and continuity. Developing robust policies for data handling in the event of vendor shutdowns is crucial to ensure data continuity, but these policies can be difficult to enforce and manage, particularly in scenarios involving multiple vendors.

One significant concern in cloud computing is the challenge of determining the physical location of data and resources. Clients often lack visibility into the policies governing control, maintenance, and security, creating a disconnect between them and service providers. Additionally, collaborations with social networking companies may compromise user privacy as preferences and interests are exchanged for financial gain, potentially violating legal standards.

The use of cryptography in cloud services raises concerns, as customers may not know who holds the encryption and decryption keys or the specific processes involved. Data integrity remains a critical focus, encompassing data transit, storage, and retrieval. Information managers are responsible for implementing safeguards that ensure the authenticity and security of data during permitted transactions.

Cloud service providers must regularly inform customers about security updates and application enhancements to maintain trust and provide reassurance. The dynamic nature of virtual machines adds complexity to security maintenance and the traceability of records, potentially affecting data record preservation.

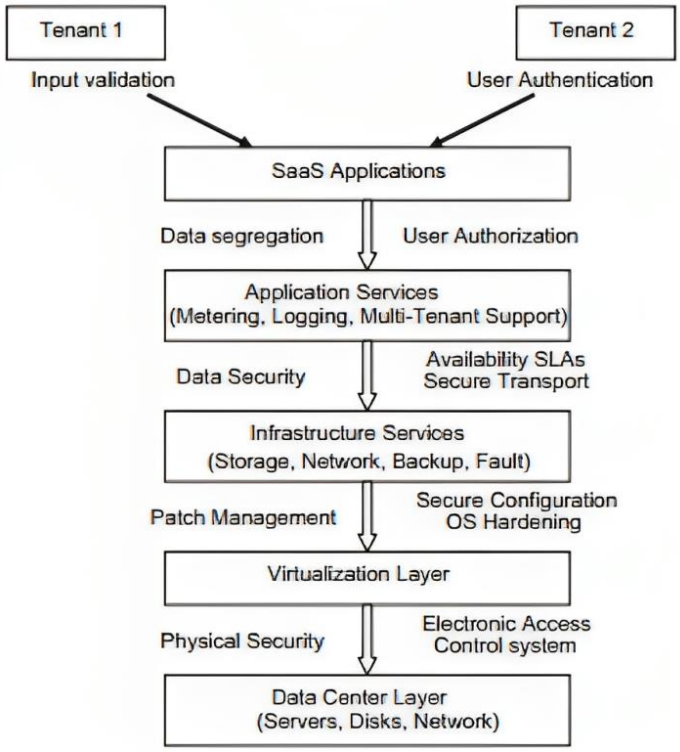

Figure 3. SaaS Security

Encryption Methods in Cloud Storage.

Encryption is crucial in securing data in cloud storage.

- **AES (Advanced Encryption Standard).** Traditionally, applied for storage data protection due to the effectiveness and reliability of the method. It is ideal for cases where there

is the need to encrypt relatively huge amounts of data. AES remains one of the most secure encryption methods, but its performance may degrade with very large datasets or high-speed data processing needs. Efficient key management and implementation practices are crucial for maintaining its effectiveness.

- **RSA (Rivest–Shamir–Adleman).** Being widely employed for protecting information exchanged and for digital signatures, RSA is significant in providing reliable connections. RSA is robust for secure key exchange and digital signatures; however, its performance can be impacted by its key size, which affects computational efficiency. Newer algorithms may offer better performance for certain use cases.
- **Homomorphic Encryption.** Enables operations to be performed directly on the encrypted data without the need to decrypt them which is privacy-preserving in cloud computing. Homomorphic encryption provides significant privacy benefits but is computationally intensive, leading to potential performance trade-offs. Practical implementations require balancing between encryption strength and system efficiency.

Recent Software Security Practices in Cloud Environments.

Some changes in cloud environments in the recent past serve to illustrate why there is a need to come up with special measures to enhance software protection. Key practices include.

- **Zero Trust Architecture.** This approach supposes that threats may be internal and external to the network; thus, user and device trustworthiness is constantly checked. Recent studies show that AI-driven tools, like those from CrowdStrike and Darktrace, enhance Zero Trust by detecting anomalies and improving response times. Blockchain-based identity systems, such as IBM's Blockchain Identity, offer decentralized, tamper-proof verification, further strengthening security.
- **Security Automation.** The role of technologies such as SIEM (Security Information and Event Management) as well as SOAR (Security Orchestration, Automation, and Response) is to automate threat analysis and remediation.
- **Identity and Access Management (IAM).** Permits only the right people to access certain information or sometimes applications through measures such as MFA and role-based access controls.

Security Recommendations.

This section proposes a three-tiered security configuration, illustrated in Figure 4. The three interconnected layers—presentation planes, cloud service center planes, and infrastructure planes—are designed to work together seamlessly. Companies considering cloud computing for their applications must evaluate and potentially revise their software development processes. Addressing key issues related to programmable devices, multi-tenancy, and essential security elements is crucial for effective cloud integration.

To overcome the challenges presented by the cloud environment, many businesses are migrating their applications to the cloud to reduce costs, enhance efficiency, and bolster the security of their application layers. Implementing a robust security framework is therefore essential. The security framework is structured into several domains.

- **Control Domain.** This domain encompasses various application-level risks. In a public cloud architecture, information is exchanged between organizations while maintaining data integrity and confidentiality.
- **Network, Connection, and End-Node Vulnerabilities.** Vulnerabilities within the cloud's accessible layer, such as those affecting networks, connections, and end-node devices, can impact middleware components. These vulnerabilities can be categorized based on their impact on data availability, integrity, or privacy.

To address these risks and uncertainties effectively, it is vital to periodically reassess the cloud infrastructure. The proposed computational framework offers versatility and scalability,

providing significant benefits for corporate entities by adapting to evolving security needs and enhancing overall cloud security. Emerging cloud architectures, such as serverless computing and containerized environments, introduce new challenges and considerations for security frameworks. Serverless computing, where the cloud provider dynamically manages the infrastructure, requires robust isolation mechanisms to prevent unintended access to functions and data. Containerized environments, while offering increased flexibility and resource efficiency, necessitate enhanced measures for container isolation and orchestration security.

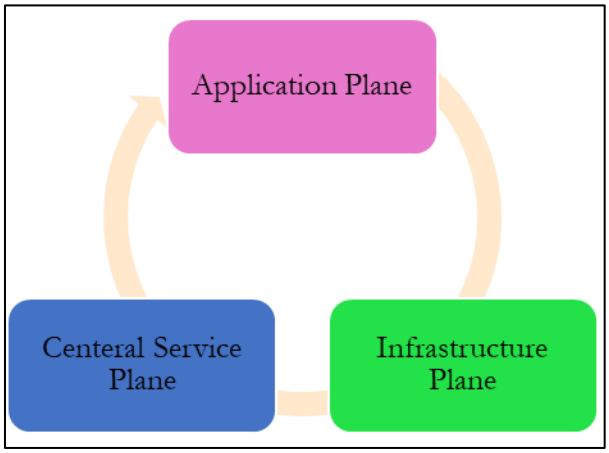

Figure 4. The 3-Tire Security Level Architecture

To accommodate these trends, the proposed three-tiered architecture should integrate additional layers of security. For serverless environments, a focus on function-level security and dynamic access controls is essential. For containerized environments, incorporating container security best practices, such as image scanning, runtime protection, and secure orchestration, will enhance the overall framework. Regular updates and adaptations of security measures to align with these new architectures are crucial for maintaining comprehensive protection.

Application Planes.

The application plane represents the ideal level for delivering outsourced software to clients. Instead of incurring upfront costs for software installation, clients can opt for a usage-based fee structure. However, this environment introduces a variety of security challenges, including end-to-end protection. Key tasks in this layer encompass scripting, XSS attacks, API security, network traffic monitoring, user identity verification, meticulous error handling, and secure communication interfaces, as illustrated in Figure 5.

Data security is a major concern within the application plane. A robust security platform is essential for comprehensive oversight and effective data protection in the cloud. Companies like McAfee and Intel have addressed these complex administrative and security challenges by providing end-device visibility. Organizational data is stored within the SaaS data centers at this layer, making service continuity a critical focus. Cloud providers are increasingly emphasizing the importance of backup systems and data replication across multiple locations to ensure service reliability.

Leading providers such as Amazon, Google Apps, and Elastic Compute Cloud (EC2) employ cryptographic techniques to enhance secure login through mechanisms like Secure Shell (SSH) access. This proactive approach is instrumental in preventing security model vulnerabilities and unauthorized access. Specific cryptographic standards are crucial in cloud storage.

- **AES-256.** Advanced Encryption Standard is popular with data storage security requirements, as it is both secure and has comparatively low-performance demands.
- **TLS (Transport Layer Security).** Secures the data transfer through the networks, which is important due to cloud service interaction with the end-users.

- **SHA-256.** A hashing standard is used and important for making sure data stored in the cloud hasn't been manipulated.

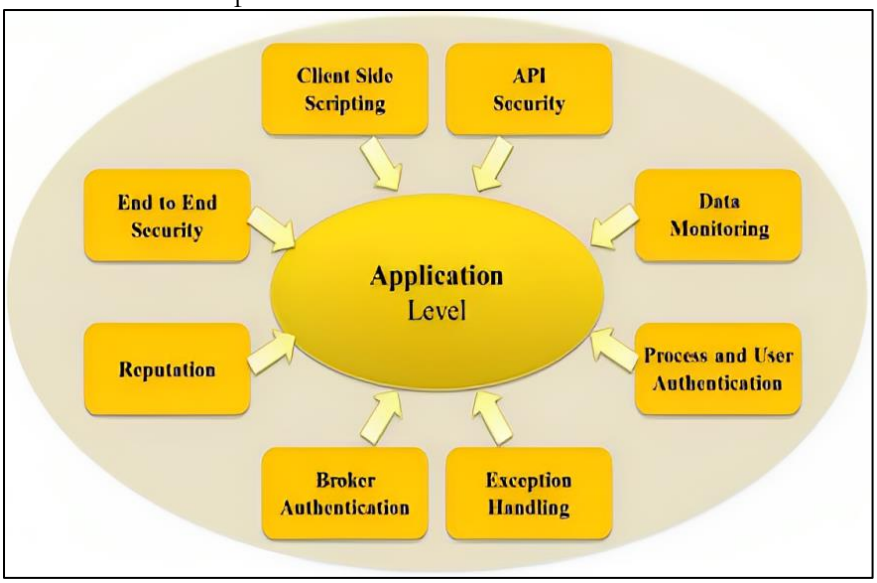

Figure 5. Factors Affecting on Application Plane

Middleware in Administrative Operations.

Middleware plays a crucial role in facilitating communication between database servers and automating services in personal computer programming. It is an integrated software solution designed to enhance efficiency for software developers in cloud-based environments. As middleware's significance grows, so do the associated security concerns. User and service authentication processes are integral to this layer, ensuring that cloud computing users in the US and Canada can adhere to service regulations with confidence, knowing their sensitive data is properly managed.

Laws and regulations now create frameworks for data sharing between organizations and external parties, outlining the procedures cloud providers must follow for data handling and storage. In the realm of middleware trust and administration, new methods have emerged, focusing primarily on trust management within cloud environments. However, there has been limited focus on evaluating the accuracy of trust ratings, highlighting a gap that necessitates further research.

Credibility benefit checking is responsible for verifying the legitimacy of customers and authorizing devices through user interfaces that serve as primary legal entry points. Despite their importance, these interfaces are highly susceptible to misuse. Thus, maintaining the integrity of protocols is essential for establishing a secure foundation for the middleware layer.

Foundation Plane.

The foundation plane encompasses the core components and structural capabilities of cloud infrastructure, allowing users to manage guest operating system configurations. It effectively handles various aspects of computing, such as bandwidth, performance, and storage accessibility. Cloud service providers often employ robust security measures to ensure data integrity, including XML encryption, Kerberos, and X.509 authentication. This plane manages critical functions like process direction and descriptor operations, as well as I/O support, pathname index maintenance, and document control within the document framework plane. To avoid obstacles at the operating system level, it is crucial to restrict and protect this section. Additionally, the infrastructure layer must support a secure and efficient process for cloud validation. Each virtual machine used in the process requires reciprocal authentication, and a strong mechanism for controlling machine availability must be implemented, as illustrated in Figure 6.

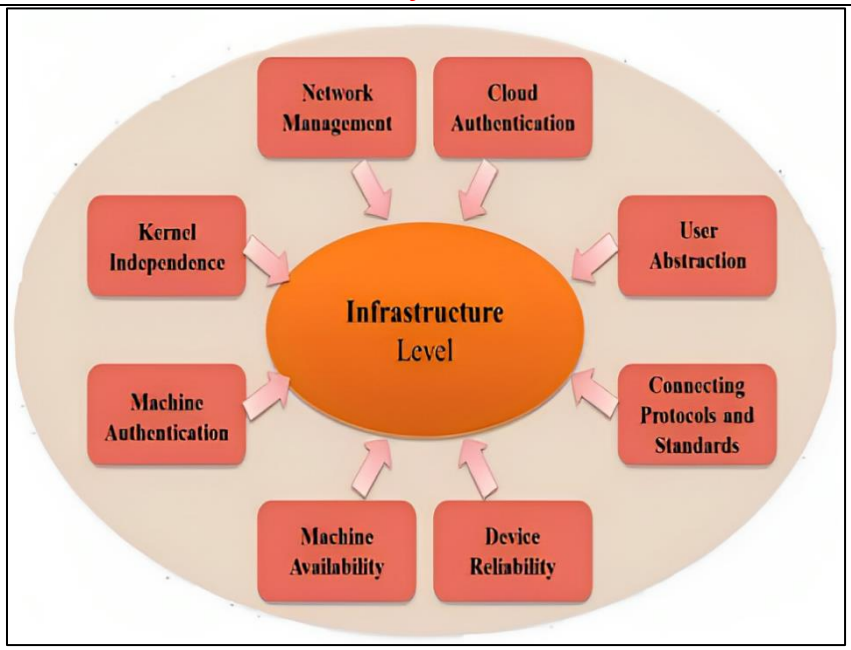

Figure 6. Components Influencing on Framework Plane

Discussion on Universal Concerns and Security Solutions.

In cloud computing, some fundamental and sensitive concerns persist, such as creating virtual machines without a hypervisor or managing data without proper organizational administration. Despite the widespread acceptance of cloud technology, ongoing research continues to address these challenges. Researchers aim to explore new security issues that have not been previously examined. This discussion will provide an overview of these areas and propose reliable and comprehensive security solutions. As cloud computing gains prominence, the visibility of security attacks increases. This includes crucial attack types such as rollback, renouncement, wrapping, session hijacking, and privilege escalation. Additionally, related research into compromised security aspects is essential.

Challenges like social engineering and insider threats impact trust, alongside issues with server management, unreliable auditing services, and misconfigured security tools in cloud storage. These concerns are exacerbated by compromised operating systems and network disruptions. Login abuse, for instance, targets legitimate users with lower security privileges, enabling them to access higher security levels than intended. Recent advancements in threat detection and mitigation include the use of AI-driven systems, which enhance the ability to identify and respond to sophisticated attacks. AI technologies can analyze vast amounts of data to detect patterns indicative of malicious behavior. However, this also introduces new risks, such as AI-driven attacks that exploit the very technologies designed to protect systems.

Preparing for post-quantum security is another critical area of focus. Quantum computing poses a significant threat to current cryptographic methods, potentially compromising data security. Researchers are developing quantum-resistant algorithms to safeguard data against future quantum-enabled decryption capabilities. These algorithms aim to provide robust protection by utilizing cryptographic techniques that remain secure even in the presence of quantum computing threats. Cloud service providers implement robust security measures and customize them to meet the diverse needs of their customers. These providers consider infrastructure requirements for applications like IoT, smart homes, and smart cities when constructing their modules. However, interoperability issues limit the effectiveness of cloud initiatives as arbiters between various cloud environments. A significant source of inspiration for intercloud initiatives is the need to circumvent vendor lock-in, which could otherwise expose clients to increased costs.

Addressing the challenges of cloud computing development requires a strong legal framework focused on data protection and privacy. Virtual Machine Monitors (VMMs), which are complex systems, demand careful setup to ensure a thorough and efficient solution. VMMs are essential for partitioning operating components and optimizing performance. They facilitate virtualized networks and communication for virtual devices, but multi-tenancy introduces security issues related to data protection, privacy, and trust. Efforts to develop security protocols for multi-tenant environments are ongoing, emphasizing the need for robust access control systems.

To advance standardization and optimization, it is crucial to incorporate relevant elements into validation and assessment tools. Legal issues in cloud computing should be reviewed, including policies and guidelines across different regions. Additionally, safeguarding sensitive information, such as health records and financial data, remains a priority. The evolution of cloud computing and sensor networks, along with cloud safety and privacy research, highlights the importance of developing effective security measures. These measures benefit both providers and customers, addressing effectiveness, cost-efficiency, and time management.

Conclusion.

Cloud-based programs represent a recent innovation offering significant benefits, including increased storage capacity, reduced costs, enhanced processing power, and greater flexibility. Cloud technology encompasses virtualization, data hosting, and popular online applications. However, it also introduces security challenges that have hindered widespread adoption. This paper has analyzed the current state of cloud security, highlighting critical issues such as identifying vulnerabilities, disrupting APIs, insider threats, web protocol vulnerabilities, and misconfigured firewalls. We examined common cloud-based attacks, classified them, and proposed recommendations and countermeasures. Future research will focus on improving network and data security, addressing recurring issues such as protocol vulnerabilities, data availability, and integrity. We will also explore algorithms to enhance system accessibility, data integrity, and classification. Additionally, we reviewed the security features of various cloud services and analyzed issues raised by each vendor. Governments play a crucial role in promoting cloud innovation to enhance performance, quality, and development. Looking ahead, future research should explore AI's role in proactive threat detection, which can enable early identification and response to emerging threats. The development of quantum-resistant algorithms is crucial for preparing against future cryptographic challenges posed by quantum computing. Additionally, blockchain technology holds promise for revolutionizing data integrity in cloud environments by providing decentralized and tamper-proof records. These advancements could significantly enhance cloud security and support the ongoing evolution of cloud-based services.

References.

[1] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, "Computational intelligence intrusion detection techniques in mobile cloud computing environments. Review, taxonomy, and open research issues," J. Inf. Secur. Appl., vol. 55, p. 102582, Dec. 2020, doi. 10.1016/J.JISA.2020.102582.

[2] M. A. R. Al Amin, S. Shetty, L. Njilla, D. K. Tosh, and C. Kamhoua, "Hidden markov model and cyber deception for the prevention of adversarial lateral movement," IEEE Access, vol. 9, pp. 49662–49682, 2021, doi. 10.1109/ACCESS.2021.3069105.

[3] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing. A Comprehensive Survey," Electron. 2022, Vol. 11, Page 16, vol. 11, no. 1, p. 16, Dec. 2021, doi. 10.3390/ELECTRONICS11010016.

[4] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," IEEE Commun. Surv. Tutorials, vol. 21, no. 4, pp. 3682–3722, Oct. 2019, doi. 10.1109/COMST.2019.2916180.

[5] S. Bharany et al., "A Systematic Survey on Energy-Efficient Techniques in Sustainable Cloud Computing," Sustain. 2022, Vol. 14, Page 6256, vol. 14, no. 10, p. 6256, May 2022, doi. 10.3390/SU14106256.

[6] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing. issues, threats, and solutions," J. Supercomput., vol. 76, no. 12, pp. 9493–9532, Dec. 2020, doi. 10.1007/S11227-020-03213-1/METRICS.

[7] S. Valluripally, A. Gulhane, K. A. Hoque, and P. Calyam, "Modeling and Defense of Social Virtual Reality Attacks Inducing Cybersickness," IEEE Trans. Dependable Secur. Comput., vol. 19, no. 6, pp. 4127–4144, 2022, doi. 10.1109/TDSC.2021.3121216.

[8] L. Da Xu, Y. Lu, and L. Li, "Embedding Blockchain Technology into IoT for Security. A Survey," IEEE Internet Things J., vol. 8, no. 13, pp. 10452–10473, Jul. 2021, doi. 10.1109/JIOT.2021.3060508.

[9] F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K. B. Kent, and S. Hakak, "Cloud computing security. A survey of service-based models," Comput. Secur., vol. 114, p. 102580, Mar. 2022, doi. 10.1016/J.COSE.2021.102580.

[10] A. Gaurav, B. B. Gupta, and P. K. Panigrahi, "A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system," Enterp. Inf. Syst., vol. 17, no. 3, Mar. 2023, doi. 10.1080/17517575.2021.2023764.

[11] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. A. El-Latif, "Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model," J. Parallel Distrib. Comput., vol. 153, pp. 150–160, Jul. 2021, doi. 10.1016/J.JPDC.2021.03.011.

[12] M. H. Sayadnavard, A. Toroghi Haghighat, and A. M. Rahmani, "A multi-objective approach for energy-efficient and reliable dynamic VM consolidation in cloud data centers," Eng. Sci. Technol. an Int. J., vol. 26, p. 100995, Feb. 2022, doi. 10.1016/J.JESTCH.2021.04.014.

[13] M. A. Elmagzoub, D. Syed, A. Shaikh, N. Islam, A. Alghamdi, and S. Rizwan, "A Survey of Swarm Intelligence Based Load Balancing Techniques in Cloud Computing Environment," Electron. 2021, Vol. 10, Page 2718, vol. 10, no. 21, p. 2718, Nov. 2021, doi. 10.3390/ELECTRONICS10212718.

[14] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, "Security in SDN. A comprehensive survey," J. Netw. Comput. Appl., vol. 159, p. 102595, Jun. 2020, doi. 10.1016/J.JNCA.2020.102595.

[15] A. Singh and B. B. Gupta, "Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms. Issues, Challenges, and Future Research Directions," https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJSWIS.297143, vol. 18, no. 1, pp. 1–43, Jan. 1AD, doi. 10.4018/IJSWIS.297143.

[16] J. K. Dawson, F. Twum, J. B. H. Acquah, and Y. M. Missah, "PRISMA Archetype-Based Systematic Literature Review of Security Algorithms in the Cloud," Secur. Commun. Networks, vol. 2023, no. 1, p. 9210803, Jan. 2023, doi. 10.1155/2023/9210803.

[17] A. Masood, D. S. Lakew, and S. Cho, "Security and Privacy Challenges in Connected Vehicular Cloud Computing," IEEE Commun. Surv. Tutorials, vol. 22, no. 4, pp. 2725–2764, Oct. 2020, doi. 10.1109/COMST.2020.3012961.

[18] W. Elmasry, A. Akbulut, and A. H. Zaim, "A Design of an Integrated Cloud-based Intrusion Detection System with Third Party Cloud Service," Open Comput. Sci., vol. 11, no. 1, pp. 365–379, Jan. 2021, doi. 10.1515/COMP-2020-0214/ASSET/GRAPHIC/J_COMP-2020-0214_FIG_009.JPG.

[19] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," Sensors 2022, Vol. 22, Page 927, vol. 22, no. 3, p. 927, Jan.

2022, doi. 10.3390/S22030927.

[20] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet. A Deep-Learning Model for Detecting Network Attacks," Proc. - 21st IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2020, pp. 391–396, Aug. 2020, doi. 10.1109/WOWMOM49955.2020.00072.

[21] W. Shi, S. Zhou, Z. Niu, M. Jiang, and L. Geng, "Joint Device Scheduling and Resource Allocation for Latency Constrained Wireless Federated Learning," IEEE Trans. Wirel. Commun., vol. 20, no. 1, pp. 453–467, Jan. 2021, doi. 10.1109/TWC.2020.3025446.

[22] N. K. Velayudhan, P. Pradeep, S. N. Rao, A. R. Devidas, and M. V. Ramesh, "IoT-Enabled Water Distribution Systems - A Comparative Technological Review," IEEE Access, vol. 10, pp. 101042–101070, 2022, doi. 10.1109/ACCESS.2022.3208142.

[23] V. Prakash, A. Williams, L. Garg, C. Savaglio, and S. Bawa, "Cloud and Edge Computing-Based Computer Forensics. Challenges and Open Problems," Electron. 2021, Vol. 10, Page 1229, vol. 10, no. 11, p. 1229, May 2021, doi. 10.3390/ELECTRONICS10111229.

[24] E. Blancaflor, B. Y. P. Saunar, T. Darrel C. Bilbao, I. H. B. Villarias, and I. Paula V. Mapue, "The Use of Cloud Computing and its Security Risks in a Philippine Education System. A Literature Review," 2023 11th Int. Conf. Inf. Educ. Technol. ICIET 2023, pp. 66–70, 2023, doi. 10.1109/ICIET56899.2023.10111146.

[25] D. R. Panda, S. K. Behera, and D. Jena, "A Survey on Cloud Computing Security Issues, Attacks and Countermeasures," pp. 513–524, 2021, doi. 10.1007/978-981-15-5243-4_47.

[26] T. Luo and Y. Shi, "Efficiently Obfuscating Proxy Signature for Protecting Signing Keys on Untrusted Cloud Servers," 2022 IEEE 25th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2022, pp. 705–710, 2022, doi. 10.1109/CSCWD54268.2022.9776312.

[27] M. Rady, T. Abdelkader, and R. Ismail, "Integrity and Confidentiality in Cloud Outsourced Data," Ain Shams Eng. J., vol. 10, no. 2, pp. 275–285, Jun. 2019, doi. 10.1016/J.ASEJ.2019.03.002.

[28] A. Pieroni, N. Scarpato, and L. Felli, "Blockchain and IoT Convergence—A Systematic Survey on Technologies, Protocols and Security," Appl. Sci. 2020, Vol. 10, Page 6749, vol. 10, no. 19, p. 6749, Sep. 2020, doi. 10.3390/APP10196749.

[29] H. K. Bella and S. Vasundra, "A study of Security Threats and Attacks in Cloud Computing," pp. 658–666, Feb. 2022, doi. 10.1109/ICSSIT53264.2022.9716317.

[30] M. Aslam et al., "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," Sensors 2022, Vol. 22, Page 2697, vol. 22, no. 7, p. 2697, Mar. 2022, doi. 10.3390/S22072697.

[31] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks. A survey of existing solutions and research challenges," Futur. Gener. Comput. Syst., vol. 122, pp. 149–171, Sep. 2021, doi. 10.1016/J.FUTURE.2021.03.011.

[32] A. Rahman et al., "SmartBlock-SDN. An Optimized Blockchain-SDN Framework for Resource Management in IoT," IEEE Access, vol. 9, pp. 28361–28376, 2021, doi. 10.1109/ACCESS.2021.3058244.

[33] T. Zhang, C. Xu, B. Zhang, J. Shen, X. Kuang, and L. A. Grieco, "Toward Attack-Resistant Route Mutation for VANETs. An Online and Adaptive Multiagent Reinforcement Learning Approach," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 12, pp. 23254–23267, Dec. 2022, doi. 10.1109/TITS.2022.3198507.

[34] I. Alam et al., "A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV," ACM Comput. Surv., vol. 53, no. 2, Apr. 2020, doi. 10.1145/3379444.

[35] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The Evolution of Quantum Key Distribution Networks. On the Road to the Qinternet," IEEE Commun. Surv. Tutorials, vol. 24, no. 2, pp. 839–894, 2022, doi. 10.1109/COMST.2022.3144219.

[36] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems. Secure Protocols, Incidents, Threats and Tactics," IEEE Commun. Surv. Tutorials, vol. 22, no. 3, pp. 1942–1976, Jul. 2020, doi. 10.1109/COMST.2020.2987688.

[37] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," Cluster Comput., vol. 24, no. 2, pp. 1235–1253, Jun. 2021, doi. 10.1007/S10586-020-03184-1/METRICS.

[38] D. Yu, Y. Jin, Y. Zhang, and X. Zheng, "A survey on security issues in services communication of Microservices-enabled fog applications," Concurr. Comput. Pract. Exp., vol. 31, no. 22, p. e4436, Nov. 2019, doi. 10.1002/CPE.4436.

[39] D. Venkata, S. Kaja, Y. Fatima, and A. B. Mailewa, "Data Integrity Attacks in Cloud Computing. A Review of Identifying and Protecting Techniques," Int. J. Res. Publ. Rev. J. homepage www.ijrpr.com, vol. 3, no. 2, pp. 713–720, 2022, doi. 10.55248/gengpi.2022.3.2.8.

[40] S. Mahdavi Hezavehi and R. Rahmani, "An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments," Cluster Comput., vol. 23, no. 4, pp. 2609–2627, Dec. 2020, doi. 10.1007/S10586-019-03031-Y/METRICS.

[41] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," Electron. 2020, Vol. 9, Page 1460, vol. 9, no. 9, p. 1460, Sep. 2020, doi. 10.3390/ELECTRONICS9091460.

[42] S. H. Gill et al., "Security and Privacy Aspects of Cloud Computing. A Smart Campus Case Study," Intell. Autom. Soft Comput., vol. 31, no. 1, pp. 117–128, Sep. 2021, doi. 10.32604/IASC.2022.016597.

[43] P. Goyal, H. Makwana, and N. Karankar, "MD5 and ECC Encryption based framework for Cloud Computing Services," Proc. 3rd Int. Conf. Inven. Syst. Control. ICISC 2019, pp. 195–200, Jan. 2019, doi. 10.1109/ICISC44355.2019.9036447.