International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Managing Security and Privacy in Cloud Frameworks: A Risk with Compliance Perspective for Enterprises

Vaidehi Shah*

Independent Researcher

Received 20 Nov 2022, Accepted 18 Dec 2022, Available online 20 Dec 2022, **Vol.12, No.6 (Nov/Dec 2022)**

Abstract

The next phase of Internet development has made cloud computing more important than traditional Internet-based computing, thanks to its scalability, cost-effectiveness, and adaptability. With more and more companies turning to cloud services to boost efficiency and adaptability, security, privacy, and privacy are rising as key concerns for widespread cloud adoption. Network security, access restrictions, data breaches, legal and regulatory compliance, and new vulnerabilities and threats are some of the important topics covered in this paper, which offers an overview of cloud computing security risks. Public cloud structures are becoming more popular among small and medium-sized enterprises, whereas private cloud structures are more popular among large organizations. Resources are virtualized in cloud computing, which is one of its core advantages but has complex security consequences. This paper shows how studies that find risks without good mitigation strategies and studies that provide technological answers without considering the bottom line are completely disconnected. Drawing on real-world scenarios and analyzing software-based and hardware-based security solutions, the study aims to better understand the dangers associated with cloud security and provide practical knowledge on how to construct a more safe and trustworthy cloud environment.

Keywords: *Cloud Security, Data Privacy, Risk Management, Regulatory Compliance, Enterprise Cloud Computing, Network security, access control, Emerging Threats, Security Techniques, Security-as-a-Service (SaaS).*

Introduction

A relatively recent development in computer science, "cloud computing" makes data, apps, and storage available over the internet rather than the user's local machine or network. This model attempts to abstract away the user's need to know how a system is physically configured and located [1]. The idea of cloud computing expands the possibilities of IT by allowing for on-demand capacity and capability improvements without the traditional IT costs associated with software licensing, massive physical investments, or adding staff. The flexibility to employ processing and storage resources on an as-needed basis is one of the many advantages of cloud computing [2]. Cloud computing is changing industries worldwide, regardless of location or type of business, by facilitating the sharing of resources to ensure consistency and by providing businesses with access to a wide range of cloud services that simplify everything from basic tools to enterprise software.

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.12.6.16

The combination of phenotypic data with genomic profiles improves the accuracy of plant disease prediction models [11]. To be more scalable and data-driven, the methods of artificial intelligence such machine learning and deep learning could be integrated into a structure for plant health management [12] [13]. Such versatile and very early diagnostic measures will, therefore, be critical for sustainable agriculture and a more extensive global food security [14].

Seed diseases are caused by pathogens invading the inside or on the seed surface and becoming active during germination [15]. Environmental conditions such as high humidity and temperature are favourable to the growth of fungi like Fusarium [16]. The contaminated seed stock serves as an agent contributing to the indiscriminate disease infection [17]. It is especially favoured by warmth and moisture in the surrounding air, Germination can also spread Fusarium wilt through infected seeds, soil and water [18] [19]. Monoculture cropping and lack of crop rotation aggravate the persistence of disease-causing organisms [20]. Furthermore, disease outbreaks are mainly favored by high Genetic Susceptibility of the plant varieties [21]. Late control becomes inevitable as

not early detection measures have been put in place [22] [23]. In addition to this, there is inadequacy in the disease surveillance systems and under-resourced laboratories [24]. In addition, it leads to the development of resistant strains of pathogens because you have overuse of chemical pesticides [25] [26]. The multifaceted nature of biological organisms and the polygenic traits of resistance characteristics make effective management strategies ever so difficult [27].

Although cloud computing promises to be revolutionary, its data security, as well as privacy issues provide strong obstacles to adoption at large-scale enterprises [3]. Cloud computing, by its very nature as a distributed, multi-tenant, virtualized architecture, can put sensitive data at risk of unauthorized access, breaches, misappropriation, leaks, cross-border transfers, API configuration errors, and ineffective access restrictions. The dynamic and elastic multiple resource provisioning also aggravates these vulnerabilities thus making it harder to maintain the same security rules [4]. Among the most critical issues of privacy, one will find policy regarding data retention, outsourced data destruction, data sovereignty, data dynamic migration, and global regulatory structures including GDPR, HIPAA, and CCPA.

Traditional security models often prove insufficient in addressing the complex, evolving threat landscape of cloud environments. Risk assessment and mitigation in such contexts requires a context-aware, service-layer-specific approach that considers the layered nature of cloud service models (IaaS, PaaS, SaaS), virtual machine isolation, API security, and user-cloud interaction dynamics [5]. Emerging analytical frameworks, such as multi-level fuzzy comprehensive evaluation, grey relational analysis, and AI-based threat detection, have shown promise in specific sectors, yet scalable, adaptable, and enterprise-grade models remain in high demand.

A growing number of organizations are migrating critical workloads to cloud providers such as AWS, Azure, and GCP, making security governance, compliance assurance, and data lifecycle management increasingly crucial for operational resilience. For these interdependent ecosystems to ensure the CIA triad, data availability, confidentiality, and integrity, it is crucial to deploy robust, automated, and flexible cloud security frameworks [6]. Security information and event management (SIEM), encryption technologies, zero-trust architecture, auditing tools for regulatory compliance, and identity and access management (IAM) are all necessary for a cloud-based enterprise's assets to be appropriately safeguarded.

Structure of the Paper

The outline of this document is as follows: An introduction to cloud computing for businesses is given in Section II. Section III discusses the difficulties associated with cloud security and privacy risks. Section IV delves into the topic of cloud computing risk management. Enterprise Cloud Security and Privacy: Trends and Challenges: A Risk and Compliance-Oriented Survey is presented in Section V. The most current literature is reviewed in Section VI, and the section on future research directions is concluded in Section VII.

Fundamentals of Cloud Computing in Enterprise Environments

Cloud computing is a huge change in business IT because it lets people use shared computing tools whenever they want over the internet. It does this by virtualizing infrastructure, which allows businesses to deploy servers, storage, and applications with minimal initial investment while providing scalability, flexibility, and cost-effectiveness. Cloud computing facilitates the adoption of new technology, speeds up innovation, and improves efficiency through the dynamic allocation of resources. In terms of fundamental service models, can look at IaaS, which provides hardware, PaaS, which provides environments for developing applications, and SaaS, which delivers software applications through the web [7]. Public, private, hybrid, and community clouds are the four main deployment models that businesses can select from; the one that best suits their requirements in terms of control, security, and compliance will determine their choice [8]. The key drivers for enterprise cloud adoption include cost reduction, faster deployment, improved collaboration, operational agility, disaster recovery, and seamless integration with advanced technologies like AI and big data, making cloud computing essential for modern business operations.

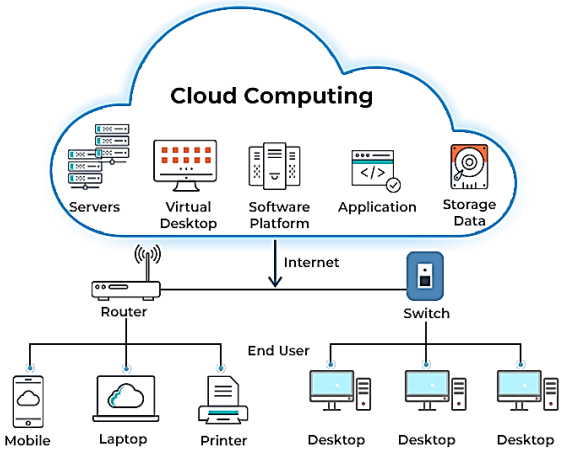

Figure 1 Cloud Computing Architecture

A model for computing in which data is stored, processed, and accessed remotely by means of an internet connection; this model includes servers, virtual desktops, software platforms, applications, and storage (Figure 1). By connecting to the cloud via a router and switch, end users are able to access cloud

resources and services with ease. This includes devices like mobile phones, laptops, desktops, and printers.

Cloud Computing Service Delivery Models

The infrastructure in the cloud and the financial rewards have become strong reasons to keep using the cloud. Scalable computing power and resources have also been made available by cloud infrastructure. Consequently, it has enabled resource flexibility, on-demand self-service, usage-based charging, and network access on demand.

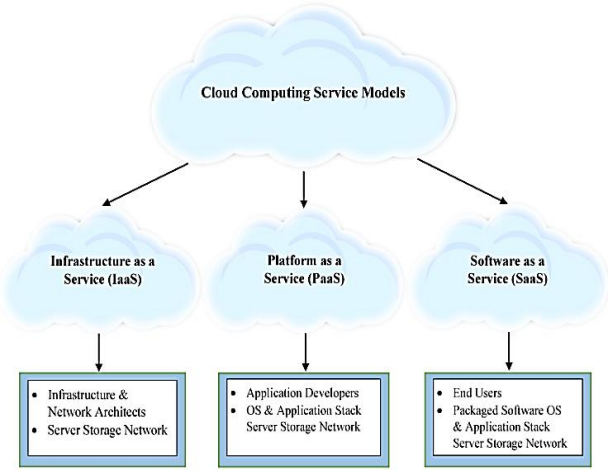

Figure 2 Infrastructure of Cloud Computing

IaaS is designed for network and infrastructure architects, whereas PaaS is for application developers, and SaaS is for end users. Each one provides a higher level of abstraction from hardware to software while still relying on server storage and network services. The cloud computing architecture, which facilitates resource availability and virtualization, is composed of three service delivery models (Figure 2). The following are some examples of cloud computing service delivery models:

Cloud Infrastructure as a Service (IaaS)

The physical administration of shared resources is made possible through IaaS. The service is offered as processing power or storage. Users may run and install any program, independent of platform or application, using the storage, processing, and networking capabilities provided by the IaaS platform [9]. Platform users may lack complete command over the platform's underlying infrastructure, but they do have complete command over the platform's software, OS, and network components once installation. In the cloud, IaaS is the foundation. The finest foundation for PaaS and SaaS is now the IaaS layer, made possible by improvements in networking, storage devices, and computing power.

Cloud Platform as a Service (PaaS)

Cloud infrastructure services, development environments, and platforms are all part of PaaS. GoogleApp Engine, Yahoo!, Dipper, and Salesforce are some instances of PaaS. The acronym "PaaS" can also refer to applications that are developed using a programming language and then hosted by a cloud provider. The development and maintenance of pre-existing applications are handled by PaaS, an abstraction of cloud services. Because it provides platform settings with all the essential development and operational qualities, PaaS is advantageous for application deployment [10]. By utilizing cryptographic co-processors, PaaS provides a secure environment where users can store and process critical data without concerns about unauthorized access. The purpose of the PaaS is to provide users a lot of control over sensitive information privacy by letting them install and modify their own software and using user data privacy techniques.

Cloud Software as a Service (SaaS)

SaaS allows customers more freedom by providing them with developer APIs and software apps like Google Maps and Bloomberg. Subscription-based SaaS models do away with the requirement for upfront software installations by charging users a flat rate [11]. Most people use a web browser to access software as a service. Applications provided by SaaS are live and accessible through customers' internet-connected devices since they are hosted in the cloud. Users of storage, operating systems, network components, and underlying infrastructure do not have control over SaaS, in contrast to IaaS. Because it allows multiple tenants to share software access controls, its multi-tenancy aspect is its main advantage.

Cloud Computing Deployment Models

There are four different architectures that organizations can use to set up their cloud computing systems. Several things affect deployment, such as who owns the data, how it is managed, where it is stored, security rules, and the type of data. The options for deployment are shown below:

Private Cloud

The private sector owns the Deployment environment, which is only used to store company data safely [12]. Private clouds are mostly run by outside companies, but they are located on-site. Only people who work for the company are allowed to access in order to keep track of who has permission and keep things safe. One example is a private data center, which a business can use to store and share client information. One strategy to ensure privacy in a private cloud is to provide users with greater control over who can access their data and to improve data security. The high equipment and energy costs are the primary issue with these establishments.

Community Cloud

A shared cloud infrastructure that is owned by multiple organizations with a common objective. Community clouds are similar to private clouds in some respects; however, in community clouds, only two organizations who prioritize user privacy and security have access to the resources and processing capacity. It costs more than the public cloud and doesn't properly control who can access data because there could be people it doesn't trust there. One of the good things about the community cloud is that it lets a fair third party check the security.

Public Cloud

Cloud service providers with substantial user bases dominate the public cloud. Examples of these companies are Microsoft Office 365, Google Apps, and AWS. The main model for resource provisioning in public clouds is the pay-as-you-go model. One major perk is the ability to buy things whenever they need them; the more they use them, the more they'll pay for them. Home customers are the majority of public cloud users. They access the providers' network from the comfort of their own homes through the internet. The fundamental problem with public cloud security is the absence of privacy and protection for data due to the cloud's very public nature. Both the transmission and the access to private information are completely unregulated. Small businesses have taken advantage of its services despite its massive security flaws since they deal with relatively little sensitive data and pose little privacy threats.

Hybrid Cloud

The interaction between several cloud providers makes the hybrid cloud service more complex, yet it is possible when private cloud owners form alliances with public cloud vendors. The public cloud's scalability and cost may be attained in this manner without putting mission-critical software at risk or exposing data to third-party applications. Fast scalability of the public cloud is one of the privacy cloud benefits of the hybrid approach. In comparison to other approaches, it provides more freedom to companies and a dramatic improvement in organizational agility. The only difference between a public cloud and a hybrid cloud in terms of security is that the latter does not expose sensitive data to the public, which poses a far greater risk to user data. The concept of controlling access to cloud resources and identities is one potential remedy for this problem.

Privacy Considerations and Data Protection with

Benefits for Cloud Adoption

Data Protection, including Privacy, is also of paramount of concern in cloud computing environments as the scale of processing, but more importantly handling, sensitive data belongs to a user of the cloud computing platform involves what would be considered distributed infrastructures. There usually is specific information with any form of personal data in the cloud that may face significant privacy infringements in case of negative management. Confidentiality and compliance also demand the application of advanced anonymization and encryption technologies, which include differential privacy, homomorphic encryption, AES, which provide their protection in transit and at rest. Also, privacy policies and user permissions are important in order to follow the regulations, including the GDPR, which enable users to manage data access and collection, as well as the way of its processing and sharing. Data are furthermore more secured as Privacy-Preserving Technologies (PPTs) such as federated learning, secure multi-party computation, and zero-knowledge proofs allow to conduct analytics and computation without sharing raw data and thus improve trust and legal adequacy within cloud ecosystems.

The major advantages and motivators of the use of clouds in enterprise Environments are as follows:

Elastic Scalability: Cloud computing allows businesses to elastically expand and contract computing resources in real time according to the current demand, and both vertical and horizontal scaling can be done without large scale physical infrastructure having to be in place.
Cost Optimization: Pay-per-use or subscription pricing reduces the overall huge capital expenditures (CapEx) and shifts IT expenses to more predictable operational expenditures (OpEx), thereby making the budget more efficient.
Enhanced Business Agility: Cloud platforms enable quicker deployment cycles where organizations can iterate, innovate and deliver products or services much faster based on the market environments.
Improved Collaboration and Accessibility: Cloud solution provides centralized access to data, making it easy to collaborate with geographically dispersed workers and even enable remote work.
High Availability and Disaster Recovery: Large cloud vendors guarantee a strong service delivery by using geographically dispersed data centers, fault-tolerance systems of automatic fallback as well as disaster recovery configurations.
Security and Compliance Capabilities: Security features which are commonly integrated with clouds services include encryption, identity and access management (IAM), regulatory compliance support.
Technological Innovation and Integration: Cloud computing facilitates the digital transformation by facilitating the deployment of cutting-edge technologies like IoT, AI, ML, and big data analytics.
Operational Efficiency: Automated resources provision, centralized management systems and the usage of infrastructure-as-code technologies helps in

less administrative burden and better operational procedures. Cloud computing can be beneficial to enhance the efficiency of enterprises by being flexible, reducing cost and innovating in terms of data security, but there will be a strong privacy and protection policies in cloud computing, which includes encryption and anonymization, just in case those policies may keep them out of the regulations.

Security and Privacy Risk Challenges in The Cloud

Data integrity acts as a foundation of trust as well as security and regulatory compliance in cloud environments, and thus it directly determines the level of user confidence, service reliability and ultimate satisfaction level. The necessity of data integrity: guaranteeing the quality and integrity of data, as well as ensuring its accessibility at all times, is of great importance when it comes to upholding a reliable connection between consumers and cloud vendors. Strict data integrity measures like data encryption, access controls, and audit tracks, go a long way beyond preventing unauthorized access, breaches of the data as well as tampering, actively enhancing the overall security architecture of cloud platforms. With respect to privacy, it is essential to keep sensitive data of a user secure against exposure, misuse or illegal sharing, particularly in multi-tenanted cloud environment where data is shared impartially and virtualized [13]. In addition, to achieve compliance with lenient security and privacy standards like the GDPR, HIPAA, and ISO/IEC 27001, which enforce secure data processing, storage, and handling requirements, it is important to ensure the data integrity. The level of compliance with these standards demonstrates a desire of the provider to protect the privacy of users and minimize legal, financial, and reputational risks. In addition to compliance, data integrity assists business continuity, in-line information access and access to disaster recovery. Finally, with clear focus on data integrity and proper security measures and privacy it is possible to provide cloud computing environment that can be robust and safe, as well as be compliant to be confident in using all the capabilities cloud computing has to offer.

The Importance of Data Security and Privacy in Cloud Computing

Cloud computing's privacy and security features are crucial in preserving the sensitive information upon which contemporary corporate operations depend. More and more organizations are relying on organizational cloud facilities for data storage, processing, and management; as a result, entities are more worried about data availability, integrity, and confidentiality. The cloud environment introduces additional dangers associated with data breaches, illegal access, insider threats, and the loss of control over sensitive information due to its decentralized and off-premises nature. There could be enormous monetary, legal, and reputational losses due to a single security breach. These dangers may be avoided with the deployment of strong security mechanisms including identity and access management (IAM), strict access control, end-to-end encryption, and ongoing threat monitoring. To add to that, maintaining stakeholder trust requires compliance with regulatory obligations including GDPR, HIPAA, and ISO/IEC 27001 [14]. A number of security models and frameworks have been put forward to address cloud-specific vulnerabilities; these have primarily concentrated on risk assessment and data security. Even more stringent security measures are needed to ensure the safety of data when emerging technologies such as RFID and the IoT are integrated into cloud infrastructures [15]. For organizations to effortlessly tap into the power of cloud computing, it is crucial to prioritize cloud security. This not only safeguards all of an organization's resources, but also instills trust, dependability, and resilience in the organization. The combination of software and hardware components strengthens the basis of data integrity, confidentiality, availability, and privacy in all three kinds of clouds: public, private, and hybrid (see Figure 3).

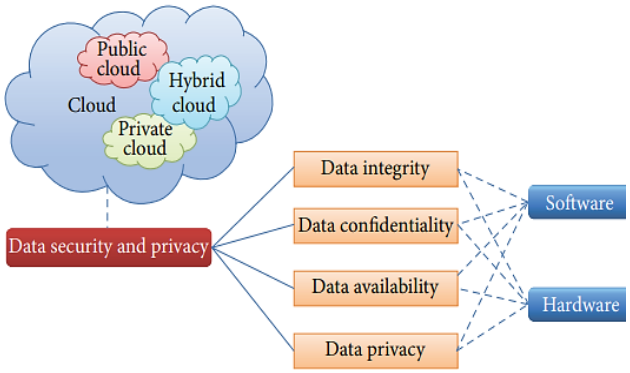

Figure 3 Organization of data security and privacy in cloud computing

These are the basic elements of data security and privacy within cloud computing systems as listed below:

Data Integrity

Data integrity allows information to be accurate, non-turned and rules out any unauthorized access to or any form of tampering with the information. In standalone systems, it is maintained through database constraints and ACID-compliant transactions [16]. In cloud computing, where data is widely distributed, integrity is preserved using techniques like RAID, digital signatures, and strong authorization mechanisms. Monitoring and third-party supervision further enhance trust. Remote verification methods, such as Proofs of Retrievability (PoR), the HAIL system, and Trusted Platform Module (TPM), enable secure integrity checks across cloud environments.

Data Confidentiality

People must take precautions to safeguard their data privacy while keeping sensitive or private information on the cloud. Data confidentiality is guaranteed by authentication and access control procedures. Cloud computing's authentication, data privacy, and access control problems may be solved by making the cloud more reliable and trustworthy. Users should exercise caution when entrusting cloud or storage service providers with sensitive information. It is extremely difficult, if not impossible, to prevent insider attacks from occurring in cloud storage. Complex requirements such as searches, concurrent updates, and fine-grained authorization are beyond the capabilities of basic encryption, which also has trouble with key management. Strictly confidential encryption is used for the following data:

Homomorphic Encryption: Protecting sensitive information is the primary goal of encryption. One type of encryption technology is homomorphic encryption. In addition to avoiding the need to decrypt data, it verifies that the outcomes of the cypher text algebraic operation match those of the clear text operation performed after encryption. Protecting sensitive information and cloud-based processes via its application is a real possibility.

Encrypted Search and Database: Since the homomorphic encryption algorithm isn't very good at what it does, researchers are mostly interested in how limited homomorphic encryption methods can be used in the cloud. A typical process is encrypted search. present an In-Memory Database encryption method to protect sensitive information in an unreliable cloud setting.

Distributive Storage: One other cool thing that could work on the cloud is data storage that is distributed. explored the privacy-related security concerns with cloud computing, namely data integrity, infiltration, and service availability. Storing data in many clouds or cloud databases is one way to guarantee data integrity.

Hybrid Technique: An approach that combines key sharing with authentication approaches is suggested to ensure the confidentiality and integrity of data. More secure methods of key exchange and authentication can improve user-provider connectivity in the cloud. Secure key distribution between customers and cloud service providers is possible with the RSA public key algorithm.

Data Concealment: The idea of data hiding for database security might likewise be utilized to keep data confidential in the cloud. Data concealing techniques inflate the perceived volume of actual data by combining it with seemingly identical bogus data.

Deletion Confirmation: Data cannot be restored once users accept deletion via deletion confirmation. There is more than one copy in the cloud for safety and ease of data recovery, which is a major problem. When users agree a data deletion, it should be done at the same time for all copies of the data.

Data Availability

Users should be able to utilize or retrieve their data in the case of calamities such as hard disc damage, IDC fires, or network failures. Additionally, they should be able to validate their data using ways other than relying on the credit guarantee supplied by the cloud service provider. This is known as data availability. Data stored on transboundary servers is a tricky issue, and cloud consumers should be aware of the local legislation that cloud providers must follow. The following are examples of cloud service providers:

Reliable Storage Agreement: The most typical issue with untrusted storage is that cloud providers may delete some of the user's update data, which is hard to detect with basic data encryption. Furthermore, it is essential for a solid storage agreement to allow for several users to make changes at the same time.

Reliability of Hard Drive: In most cloud storage solutions, the hard disc is still the main storage medium. A key component of cloud storage is the dependability of hard drives. Using data collected from previously used hard discs, Pinheiro et al. investigated their mistake rate. However, they did find that hard disc error rates cluster strongly and are unrelated to operating temperature or frequency.

Data Privacy

The capacity to conceal one's identity or one's information and reveal it selectively is what mean when talk about privacy. There are several components to privacy. Some subjects may be more worried about the disclosure of future or present information than they are about the disclosure of past information. While users could feel more at ease if their friends can ask for their information manually, they might be less than thrilled about receiving regular and automated reminders. Instead of a specific spot, the user can choose an ambiguous zone to represent their data. The following are some subcategories into which the privacy issues fall, depending on the specific cloud scenario:

Service Abuse: Aggressors commit service abuse when they take advantage of a cloud service to steal information or harm other users. One consequence of deduplication technology's widespread use in cloud storage is that identical data is frequently saved once but shared by numerous users.

Averting Attacks: The ability to pool a large number of resources across the Internet is what makes cloud computing possible. Any cloud service worth its salt will have defenses in place to prevent DoS assaults.

Identity Management: Cloud computing's accessibility to several web-based apps is one of its primary advantages. A trusted third party increases the security risk, notwithstanding its benefits. Cloud security may be jeopardized due to user heterogeneity and the reliability of the third party.

Challenges in Data Integrity with in Cloud Computing Environments

The integrity of data stored in the cloud is susceptible to a number of threats. These are among the most important concerns:

Data Breaches and Unauthorized Access: Hackers commonly target cloud infrastructures because they store large amounts of sensitive data. When unauthorized individuals get access to, alter, or steal critical data, it can compromise data integrity.

Data Corruption and Loss: Cloud storage has the potential of corrupting or losing data due to a number of reasons, some of which are the hardware failure, software error, network challenges, and natural catastrophes. The data integrity process entails protection of data against possible threats as well as setting up data backup and recovery protocols.

Shared Responsibility Model: Managed through a shared responsibility model, a small part of the risks and potential issues of data integrity and security are allocated to the cloud provider and the user. Misunderstandings or mis responsibilities can easily result in vulnerabilities and data integrity violation.

Insider Threats: Accidental or deliberate insider threats can be very detrimental in data integrity in the cloud. People who access the cloud resources, including individuals like the employees, contractors, or any other insiders, are in a position to abuse their privileges whether willingly or unwillingly, which may defeat the integrity of the data.

Complexity of Distributed Systems: Cloud environment is complex because it is distributed in nature, and this poses some challenges in ensuring the data is consistent and has integrity across many data centers, locations and services. In order to guarantee maintenance of data integrity in such set-ups, it is imperative to introduce effective content coordination and synchronization technique.

Data Migration and Interoperability: Migration of data between different cloud providers or migration of on-premise to cloud could also become a point of threat to the integrity of the data. Data migration operations are an essential aspect of preventing the potential risks of losing data, corruption of data, or their misuse associated with the application of inadequate planning or implementation.

Lack of Transparency and Visibility: Cloud customers may not have the transparency and access to security safeguards and other procedures in data integrity used by cloud providers. The absence of knowledge on the means of keeping data as well as storing and protecting data could interfere with confidence and trust in cloud services.

Risk Management in Cloud Computing

The management of risk as used in cloud computing refers to a proactive way of identifying risks, evaluating risks, and limiting risks that are actual to cloud based conditions. Some of the threats that organizations experience since they use cloud services commonly include data breaches, threat to service, unauthorized use and compliance [17]. Good risk management requires that specific plans that will help curb such threats should be drawn up with the impacts of each risk maintained on levels that can be scaled down to reasonable levels in order to safeguard business survival and the security of data. It helps make better decisions, keep the assets safe, improves the efficiency of operations and enhances the security of systems and in the long run the organizations are able to think ahead of the problems and act on them instead of acting after the damage is done.

Risk Management Frameworks in Cloud Computing

A framework for risk assessment an early risk assessment approach suggested shifting some responsibility to the cloud provider or a reliable third party, although it was only ever meant to assist cloud users. Nevertheless, the method does not acknowledge that cloud providers regulate and maintain the infrastructure and might not be allowed to share specific security models and processes as that would be dangerous to them given that they could fall prey to malicious parties [18]. Conversely, other frameworks have suggested that only cloud providers should conduct risk assessments, neglecting the crucial role of cloud consumers in the process. In reality, effective risk management in cloud computing requires a collaborative approach, where both providers and consumers share responsibility for identifying, evaluating, and mitigating risks within their respective domains [19]. Figure 4 shows the five main steps that make up this framework: self-evaluation of user requirements, examination of cloud service providers' desktops, assessment of risk, review by third-party organizations, and continual monitoring.

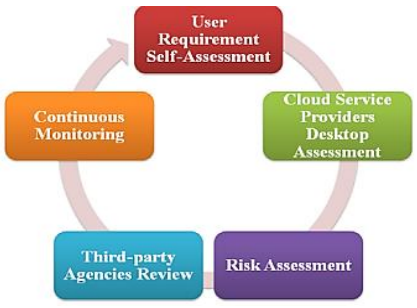

Figure 4 The Cloud Computing Risk Management Framework

These are the five basic processes of risk management in cloud computing environments are given below:

User Requirement Self-Assessment

Cloud computing services, service models, deployment types, and necessary security levels are all aspects of a

system that users should consider when doing a requirement self-assessment. Determining the level of security required from the cloud platform should be the top priority. Levels are typically used to categorize 0073 this. Authentication, data integrity, discretionary access control, and auditing capabilities are some of the more sophisticated security features that are displayed at higher levels. The second thing that consumers need to do is figure out what features they need, because that will affect which service providers they can go with. After that, they can choose the right cloud service model, such SaaS, PaaS, or IaaS, for their needs. Choosing a deployment model that meets the system's security requirements is the next stage. The NIST states that there are four types of clouds: private, public, hybrid, and community. Due to the unique control over the architecture, private clouds are perfect for systems that demand a high degree of security. Having said that, they are more expensive. Public cloud shared infrastructure, on the other hand, is a solid choice for less important systems. Based on their specific needs for deployment, service, and security, users can use these reviews to narrow down their pool of potential cloud providers.

Cloud Service Providers Desktop Assessment

Once a shortlist of potential cloud service providers has been created, the next step is to conduct a desktop assessment. This phase involves analyzing and evaluating the cloud service plans offered by each applicant, as well as their prior performance in terms of security and the associated security risk. The user requirements are usually included to these services plans and normally they contain particulars like the platform of cloud chosen, scope of services, specification of the data centers, hardware and the software infrastructure, security measures, approaches toward migration, user isolation strategies, data backup procedures, service termination policies as well as the responses to incidents. One of the most important parts of this assessment is the analysis of the historical security situation of the providers that helps to determine the risks basing on past security incidents [20]. These are classified as either adversarial which are caused by external threat such as hackers or cyber-criminal gangs or non-adversarial which are caused due to the natural disasters, system failures or accidental human errors and so forth. The two types are rated on the possibilities that they happen and the consequences they can bring in regards to its occurrence. A five-point scale from "very low" to "high" is used to qualitatively categorized the likelihood of incidents in order to facilitate this study. Table I lays forth the criteria for determining whether an occurrence is adversarial (A) or non-adversarial (NA), meaning that their meaning changes accordingly. By following this systematic examination, provides a detailed risk profile for every supplier, which can help it make better decisions.

Risk Assessment

Cloud providers often go through seven steps in their risk assessment process: documenting the evaluation, identifying assets, threats, vulnerabilities, current security measures, and risk analysis. In this short example will show how to do a risk assessment by identifying assets, threats, and vulnerabilities. Assets: Cloud computing systems incorporate several assets. According to the ENISA report [21]When assessing the safety of cloud computing, users have the option to reclassify these categories.

Risks are defined as factors that could lead to the alteration, destruction, or disruption of any service or valuable asset stored in the cloud, whether it belongs to users or providers. When doing a risk assessment, it is crucial to consider the cloud service environment and the potential impact on both consumers and providers of cloud services when doing a threat analysis.

There are two basic categories of vulnerability: technological and managerial. Problems with data, applications, systems, networks, and physical layers are all examples of technical vulnerabilities. Technology management pertains to the management of certain technological tasks, while organizational management is concerned with environmental management. These two branches of management are liable to different degrees. System or operating system vulnerabilities, untrusted applications, and other similar issues are common and not unique to cloud computing. There are a number of security concerns specific to cloud computing, including issues with user provisioning, authentication, authorization, and accounting; the lack of resource separation; the safe handling of sensitive data; and many more.

Third-Party Agencies

Employing third-party organizations to examine the procedure is important to ensure the regular operation and security of cloud services. Trustworthy security evaluation entities, such as review boards and expert committees, should unsurprisingly serve as the third parties. Figure 5 depicts the process, which involves several organizations, including users, experts, third-party reviewers, and cloud service providers.

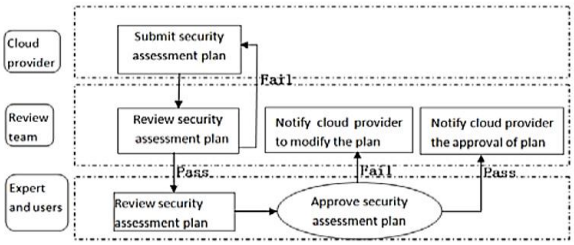

Figure 5 Organizations in the Cloud environment

Continuous Monitoring

The continuous monitoring procedure entails keeping an eye on the continuing risk assessment and

modifying the program as necessary to account for changes in the environment.

Risk Management Pros and Cons

The complexity of the cloud computing environment makes it such that many elements can affect how successful a risk management framework is, and there is no such thing as a perfect system [22]. Table I below compares and analyses the several proposed security risk management frameworks for use in cloud computing environments.

Table 1 Risk Management Frameworks Pros and Cons

Aspects	Pros	Cons
Risk Assessment Approach	Enables identification and analysis of cloud-specific risks. Supports comparative evaluation across cloud providers.	Often focuses only on assessment, ignoring other stages like risk treatment and monitoring. May require complex data and expertise.
Methodology (Qualitative / Quantitative / Hybrid)	Hybrid methods reduce bias and combine precision with flexibility. Quantitative approaches provide measurable results.	Qualitative methods limit cost-benefit analysis. Quantitative methods may be costly, complex, and require advanced tools.
Consumer Involvement	Enhances transparency and trust. Ensures risk decisions reflect user concerns.	High involvement may complicate or delay processes. Often lacks involvement in final risk treatment or acceptance.
Provider vs Consumer Perspective	Provider-centric models support infrastructure-level security, and Consumer-focused models prioritize data and service risks.	Overemphasis on one side may overlook the responsibilities or risks of the other. Balanced consideration is often missing.
Risk Identification and Coverage	Frameworks that identify threats, vulnerabilities, and assets provide comprehensive protection.	Some frameworks skip risk identification or narrow their focus.
Adaptability and Flexibility	Dynamic models enable updates based on evolving threats. Supports cloud-specific environments.	Static models may ignore emerging or context-specific risks. Inflexible critical areas may miss new vulnerabilities.
Third-Party Involvement	Independent assessments can enhance objectivity and trustworthiness.	Adds complexity and may reduce consumer control. May not align with specific organizational needs.
Cost-Benefit Analysis	Helps in prioritizing risk controls based on value and impact.	Often not supported in qualitative-only frameworks. Difficult to perform without reliable risk valuation methods.

Trends and Challenges in Enterprise Cloud Security-Privacy: A Risk and Compliance-Oriented Survey

Virtual instance management in the cloud is an ever-evolving problem that calls for constant investigation, evaluation of security, and preventative measures. It becomes increasingly challenging to centrally manage assets when cloud workloads are distributed over numerous sites. The following are examples of difficulties:

Challenges in Securing Cloud Computing

Figure 6 depicts some of the major obstacles that businesses face when trying to guarantee the accuracy of data stored in the cloud.

Several of these threats to privacy and security in the cloud, as well as issues with compliance, are listed below:

Data Transmission Security: Protecting client data while it travels to the cloud is a top priority [23]. Secure and private data transmissions require robust encryption methods, dependable network communication channels, and safeguards against unauthorized data tampering or interception.

Data Storage Security: Once the data gets into the cloud, it is saved in scattered servers and data centers. Data integrity must be ensured by protection against hardware failure, unauthorized access and data corruption during data storage. In order to protect against these threats, measures such as encryption of data, access controls, redundancy and data integrity ought to be used.

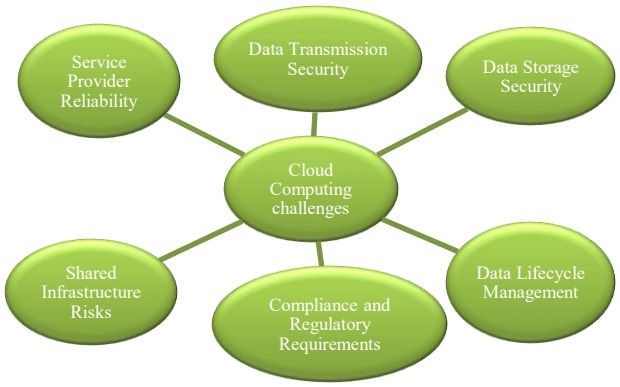

Figure 6 Challenges of Cloud Computing

Shared Infrastructure Risks: Multi-tenancy or sharing of the same physical hardware by multiple users and tenants is common in cloud computing. This general environment increases the likelihood of data leakage, internal attacks, and vulnerabilities that are based on underlying infrastructure to be attacked. In order to contain such risks and uphold the integrity of data, effective isolation mechanisms, access control and monitoring systems should be employed.

Service Provider Reliability: Organizations rely on cloud service providers to ensure that there is

availability of the cloud services and data integrity. Nonetheless, the integrity of data can be compromised due to breaches by the providers, outages, or service interruption. Enforcement of backup and recovery, contingency plans and service level agreements (SLAs) might help to minimize effects of provider related risks on the integrity of the data.

Data Lifecycle Management: The fact that data has to be managed through all stages of its life cycle, including its creation, storage, processing, and destruction, hinders its integrity maintenance. In order to maintain the data integrity over its full lifecycle, organizations need policies and procedures about data categorizing, controlling access to data, its encryption, and safe destruction.

Compliance and Regulatory Requirements: Industry practice and data protection requirements pose an additional challenge to companies operating in controlled industries. Strong controls related to security including tracking and documentation of the processes are essential toward enforcing data integrity and meeting the law requirements, including the GDPR, the HIPAA, and PCI DSS, among others.

The challenges of data integrity in cloud computing require a comprehensive approach that includes organizational, technological and legal preventive measures. By enacting thorough security strategies, barriers, data encryption, surveillance systems, and observe the excellent practices, enterprises can cut the chances of damaging data integrity and maintain confidence in their cloud setup.

Emerging Trends with Solutions of Cloud Data Security at Risk Compliance

As cloud computing expands with adverse velocity, emerging trends are transforming the organizations in its data vulnerability and risk compliance strategies. One of them is the combination of AI and ML that is vital to real-time threat detection, anomaly analysis, and predictive security operations. There is also a growing use of Zero Trust Architecture that reduces the implicit trust of the network and protects every layer using robust identity verification. Moreover, confidential computing enables one to process encrypted data in encrypted environments and, hence, protect sensitive workloads as those processes occur.

Organizations are engaging automated tools to track compliance with regulation such as GDPR and HIPAA to address growing needs of compliance and curb risks. The blockchain technologies are being investigated with a secure audit information and cloud-native frameworks are enhancing visibility, access and enforcement of policy. These solutions would improve cloud security and aids in regulatory authorization in complicated settings [24]. Cloud computing has developed numerous problems and threats, and that is why several solutions to the problems have been sought and consequently developed. There are very many solutions that are proposed and in operation in the circumstances of these problems or threats. The following are the resolutions to the cloud data security solutions discussed below:

Encryption: The use of strong encryption systems to secure data both over the network and storage. This involves securing sensitive information through encryption, prior to its upload to cloud as well as its transmission and storage processes.

Access Controls: restricting access to sensitive data, implementing authentication prescriptions, and access restrictions at the granular level. Authored users are the only ones who have access rights to read and change data due to such technologies as IAM, MFA, and RBAC.

Data Validation and Integrity Checks: verifying the correctness of data through means of hash functions, digital signatures and checksums. Regular checks of the integrity of data also ensure that it is credible and that any alteration of the data has been prevented and as well help in identifying any form of illegal manipulation or corruption.

Audit Trails and Logging: installing comprehensive log and auditing policies to track the activity, data usage, and modification of the system. Audit logs allow the organizations to detect security events, derive suspicious activities, and preserve data integrity.

Data Replication and Redundancy: in order to ensure fault tolerance and high availability, employing redundancy and data replication methods is an important practice. The data losses caused by the malfunctions of the hardware, natural disasters or other inconveniences are reduced when the duplicated copies of the data have been saved in different geographical locations.

Continuous Monitoring and Threat Detection: Incorporation of intrusion detection systems and monitoring tools to detect suspicious activity and likely security threats in the cloud environments. With real-time detection of the threat, organizations can protect the integrity of data and respond to security issues promptly.

Compliance and Governance Frameworks: upholding legal standards and industry best practices in the security and integrity of data. Through compliance regimes, such as ISO 27001, GDPR, HIPAA, and SOC 2, compliance frameworks make sure that data processing practices follow legal and regulatory practices.

Vendor Due Diligence: performing due diligence in the security practices, certifications, and best industry practices of cloud service providers. The risks of using third-party cloud services identified in terms of the data integrity are decreased by the choice of trustworthy suppliers that have effective security measures.

Employee Training and Awareness: Providing entire training and awareness programs, which will inform the staff members on regulations, operations, as well as best practices regarding data security. By developing a security-savvy culture in the firm, there are fewer

chances of insider attacks and human error in violating the integrity of data given the environment in which people work.

Literature Review

In this section, an overview of the literature on Security and Privacy in The Cloud: A Risk and Compliance Perspective to Enterprises was provided; several approaches, and integration issues were identified, and the future trends were also mentioned. Key approaches, key findings, challenges, and future directions will be outlined in Table II and will provide the reader with information about the current trends and gaps in research.

Arora, Gera, and Saxena (2021) explain the problems with implementing Cloud-based Enterprise Resource Planning (ERP) systems in healthcare settings, such as hospitals, and the associated security concerns around the possible usage of patient data in these systems. It goes on to detail the challenges that came up during and after the SaaS (Software as a Service) installation, and offers suggestions for how to get over them. Also included in this study is a comparison of cloud usage before and after hospital implementations, as well as an analysis of the benefits and drawbacks of cloud-based ERP in healthcare, and a determination of whether or not such an implementation can effectively and affordably monitor and treat patients. A survey methodology was used to gather the data. The results of the survey show that ERP software hosted in the cloud is reliable and allows for secure data storage thanks to the use of cutting-edge encryption methods. The advent of cloud-based applications has revolutionized the way businesses operate by freeing up internal resources formerly dedicated to server administration, upgrades, and upgrades to disaster recovery, business continuity planning, and other software [25].

Abioye et al. (2021) the goal of this assessment is to determine the degree to which security risk management is integrated into the different BPLC procedures for protecting cloud-based business processes. It will also examine the frequency of security risk standards usage, the cloud security risk classification scheme, and the risk assessment model's reliance on an existing risk analysis technique. In order to achieve these goals, this study analyzed the best practices for reducing security risks in cloud-based business processes in great detail. Eleven separate online databases were combed through to find the selected articles. A total of 1,243 objects were found by us. After 93 articles were reviewed using the selection criteria, 17 were found to warrant a more comprehensive evaluation. A total of seventeen percent of the business process lifecycle alternatives considered incorporated security risk management into some stage. The other methods failed to [26].

Alouffi et al. (2021) analyzed the current literature on the topic of cloud computing security, including studies that have examined potential risks, difficulties, and weaknesses. This SLR combed through the widely-used digital libraries' holdings of academic articles released between 2010 and 2020. After a thorough review of all published studies, they settled on 80 papers to address the research topics. Based on the results of this SLR, cloud computing services face seven serious security risks. Among the most talked-about issues in the selected literature were data leaks and tampering, according to the results. Data intrusion and storage in the cloud were more sources of security worry. The results of this SLR show that cloud service providers and their clients still face challenges when trying to outsource consumer data. Its study document highlighted blockchain technology as a possible ally to calm concerns around data security. The findings of the SLR should guide future studies in ensuring the accessibility, authenticity, and privacy of data [27].

Jiang et al. (2021) identify the difficulties and potential security threats associated with network function outsourcing (NFV) in a cloud environment by doing an exhaustive literature review of the topic, paying particular attention to privacy and security concerns. Afterwards, it compares and contrasts current secure network function outsourcing systems based on their features, efficiency, and level of security. Their discussion of potential avenues for further study serves as a final section. With the help of network function virtualization (NFV), communication facilities and the availability of network functions can be made more programmable and flexible. At the same time, thanks to developments in cloud computing, there has been a shift towards using cloud service providers to outsource network operations, such as virtualization, and away from in-house IT departments. Several security and privacy issues have been brought up by the promising practice of rerouting communication traffic to a third-party source. While traditional end-to-end encryption does a good job of protecting data while in transit, it makes data less useful in the end [28].

Jaatun et al. (2020) prioritize the role of accountability in data management, particularly in relation to cloud computing. The ability and readiness of a reliable cloud service to carefully manage the data of other individuals is a crucial component of this concept. In this paper, define accountability in the context of cloud computing and present a conceptual model for the provision of accountability for cloud services. Responsibility can thus be considered at higher levels of abstraction, such as in the context of its actual implementation, thanks to this. To avoid potential problems with account provisioning and verification, the system is based on the tenets of strong responsibility. Data subjects, cloud customers, and regulators are all parties involved in the cloud ecosystem, and it is possible that they will need to see different types of accountability proof and notifications [29].

Yang, Xiong and Ren (2020) investigate cloud storage security and privacy concerns, data encryption methods, and relevant countermeasures. In particular, they begin with a general introduction to cloud storage, covering such topics as definition, categorization, architecture, and uses. Second, they break down the needs and obstacles of cloud storage security and privacy protection in great depth. The third part is a synopsis of data encryption techniques and technology. Lastly, they go over a number of unanswered questions about cloud data security[30].

Table 2 Literature summary on Managing Security and Privacy in the Cloud: A Risk and Compliance for Enterprises

Author(s)	Study Focus	Approaches	Key Findings	Strategies	Limitations	Challenges
Arora, et.al. (2021)	Problems with healthcare cloud ERP implementation and security	Survey methodology on hospitals using SaaS ERP	Cloud-based ERP enhances cost-efficiency and patient care; uses strong encryption; less need for hardware maintenance	Emphasized secure data storage, encryption, and reduced infrastructure burden	Limited to healthcare; lacks technical depth in security analysis	Data security, implementation barriers, server maintenance overhead
Abioye et al. (2021)	The BPLC-wide incorporation of security risk management	Thorough examination of the existing literature; assessment of 1243 papers, including 17	Only 17% of models integrated risk management at any BPLC phase	Recommends deeper integration of risk management standards in all BPLC phases	Low integration across BPLC; the majority of models lack comprehensive coverage	Incomplete risk integration across the lifecycle; lack of a unified approach
Alouffi et al. (2021)	Cloud computing security: potential risks and obstacles	Systematic Literature Review (SLR); 80 selected studies (2010–2020)	Identified 7 key threats; data leakage/tampering most discussed; Blockchain seen as future solution	Proposed Blockchain to enhance confidentiality, integrity, and availability (CIA)	General overview: lacks implementation analysis for proposed solutions	Data outsourcing risk, confidentiality, integrity, and availability
Jiang et al. (2021)	Security/privacy in Network Function Virtualization (NFV) outsourcing	Comparative survey of NFV models and secure outsourcing schemes	Outsourcing reduces cost but raises privacy risks; end-to-end encryption impacts usability	Comparative analysis of outsourcing schemes: the need for a balance between privacy and utility	Trade-off between encryption and usability; lacks real-world deployment validation	Outsourced traffic vulnerabilities, secure processing
Jaatun et al. (2020)	Accountability in cloud information management	Conceptual modeling of accountability in cloud systems	Importance of provider transparency and responsibility; accountability must be auditable	Conceptual model for cloud accountability, with operationalization suggestions	Conceptual only; no empirical validation or industry adoption evidence	Demonstrating responsibility, verifying cloud provider behavior
Yang, et. Al. (2020)	Review of data security and privacy issues, encryption techniques, and countermeasures in cloud storage systems	Thematic analysis covering cloud storage architecture, security concerns, and encryption methods	Identified major security threats, categorized encryption methods, and outlined privacy protection demands	Symmetric/Asymmetric Encryption-Homomorphic, Encryption-Attribute-Based Encryption, Access control mechanisms-Multi-level security models	Lacks empirical validation-Does not compare performance of security methods-Focuses more on theoretical aspects	Rapid evolution of threats-Balancing usability with strong encryption-Scalability of protection methods- Key management complexities

Conclusion and Future Work

Cloud computing's adaptable, scalable, and inexpensive design has, in the end, led to its meteoric rise in popularity in recent years, with many companies shifting their focus to it. The greatest obstacles to its wider use, however, are worries about data security and privacy, particularly in public cloud settings where the likelihood of data breaches and illegal access is greater. To minimize these challenges, organizations are forced to engage in a holistic data integrity perspective which should involve technological, organizational or regulatory aspects. The paper will examine some of the major methods towards improving data privacy as well as security in the cloud setting and these will be based on secure storage and data usage. It also incorporates a framework of cloud security management that presents the evaluation of the user and provider, and the third-party evaluation of compliance and safety of the application. A rather promising user-centric model is Security-as-a-Service (SaaS) which is more transparent and involves more control in the protection of data. In future work on coming up with more advanced protection models

where encryption and data concealing approaches are incorporated to increase the level of trust as well as resilience in cloud computing.

References

[1] J. Thomas, K. V. Vedi, and S. Gupta, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," J. Emerg. Technol. Innov. Res., vol. 8, no. 9, 2021.

[2] U. A. Butt et al., "A review of machine learning algorithms for cloud computing security," Electronics (Switzerland). 2020. doi: 10.3390/electronics9091379.

[3] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," Procedia Comput. Sci., vol. 125, pp. 691–697, 2018, doi: 10.1016/j.procs.2017.12.089.

[4] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," J. Adv. Dev. Res., vol. 11, no. 1, 2020.

[5] Z. Li, Z. Tang, J. Lv, H. Li, W. Han, and Z. Zhang, "An information security risk assessment method for cloud systems based on risk contagion," in 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), IEEE, Jun. 2020, pp. 83–87. doi: 10.1109/ITOEC49072.2020.9141852.

[6] M. Alenezi, "Safeguarding Cloud Computing Infrastructure: A Security Analysis," Comput. Syst. Sci. Eng., vol. 37, no. 2, pp. 159–167, 2021, doi: 10.32604/csse.2021.015282.

[7] S. O. Kuyoro, F. Ibikunle, and A. Oludele, "Cloud Computing Security Issues and Challenges," Int. J. Comput. Networks, vol. 3, no. 5, 2011.

[8] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.

[9] M. E. Suliman, "A Brief Analysis of Cloud Computing Infrastructure as a Service (IaaS)," Int. J. Innov. Sci. Res. Technol., vol. 6, no. 1, pp. 1409–1412, 2021.

[10] A. J. Ferrer, D. G. Pérez, and R. S. González, "Multi-cloud Platform-as-a-service Model, Functionalities and Approaches," Procedia Comput. Sci., vol. 97, 2016, doi: 10.1016/j.procs.2016.08.281.

[11] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," in 2010 Sixth International Conference on Semantics, Knowledge and Grids, IEEE, Nov. 2010, pp. 105–112. doi: 10.1109/SKG.2010.19.

[12] S. Goyal, "Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review," Int. J. Comput. Netw. Inf. Secur., vol. 6, no. 3, pp. 20–29, Feb. 2014, doi: 10.5815/ijcnis.2014.03.03.

[13] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 2, 2019.

[14] L. Kacha and A. Zitouni, "An Overview on Data Security in Cloud Computing," in Advances in Intelligent Systems and Computing, vol. 661, no. 1, 2018, pp. 250–261. doi: 10.1007/978-3-319-67618-0_23.

[15] J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," Int. J. Res. Anal. Rev., vol. 8, no. 3, pp. 874–879, 2021.

[16] S. Aldossary and W. Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, 2016, doi: 10.14569/IJACSA.2016.070464.

[17] S. Tanimoto et al., "A Study of Risk Assessment Quantification in Cloud Computing," in 2014 17th International Conference on Network-Based Information Systems, IEEE, Sep. 2014, pp. 426–431. doi: 10.1109/NBiS.2014.11.

[18] A. E. Youssef, "A framework for cloud security risk management based on the business objectives of organizations," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 12, pp. 186–194, 2019, doi: 10.14569/ijacsa.2019.0101226.

[19] M. Medhioub, M. Hamdi, and T. H. Kim, "Adaptive risk management framework for cloud computing," in Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 2017, pp. 1154–1161. doi: 10.1109/AINA.2017.143.

[20] Q. Duan, "Cloud service performance evaluation: status, challenges, and opportunities – a survey from the system modeling perspective," Digit. Commun. Networks, vol. 3, no. 2, pp. 101–111, 2017, doi: 10.1016/j.dcan.2016.12.002.

[21] H. J. Kim, "Three Approaches to Risk Management in the Cloud," Inf. Resour. Manag. J., vol. 35, no. 1, pp. 1–12, Dec. 2021, doi: 10.4018/IRMJ.287908.

[22] R. Alosaimi and M. Alnuem, "Risk Management Framework for Cloud Computing : A Critical Review," Int. J. Comput. Sci. Inf. Technol., vol. 8, no. 4, pp. 01–11, Aug. 2016, doi: 10.5121/ijcsit.2016.8401.

[23] M. Sen and S. S. Choudhury, "Security and privacy issues for cloud computing and its challenges," Adv. World Inf. Eng., vol. 4, no. 2, pp. 62–66, 2017, doi: 10.18280/rces.040204.

[24] B. A. Alenizi, M. Humayun, and N. Z. Jhanjhi, "Security and Privacy Issues in Cloud Computing," J. Phys. Conf. Ser., vol. 1979, no. 1, 2021, doi: 10.1088/1742-6596/1979/1/012038.

[25] R. Arora, S. Gera, and M. Saxena, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," in 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 458–463.

[26] T. Abioye, O. Arogundade, S. Misra, K. Adesemowo, and R. Damaševičius, "Cloud-Based Business Process Security Risk Management: A Systematic Review, Taxonomy, and Future Directions," Computers, vol. 10, no. 12, Nov. 2021, doi: 10.3390/computers10120160.

[27] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," IEEE Access, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[28] P. Jiang et al., "Building In-the-Cloud Network Functions: Security and Privacy Challenges," Proc. IEEE, 2021, doi: 10.1109/JPROC.2021.3127277.

[29] M. G. Jaatun, S. Pearson, F. Gittler, R. Leenes, and M. Niezen, "Enhancing accountability in the cloud," Int. J. Inf. Manage., vol. 53, Aug. 2020, doi: 10.1016/j.ijinfomgt.2016.03.004.

[30] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," IEEE Access, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.