Threats in Cloud Computing System and Security Enhancement

Mohammed Khodayer Hassan Al-Dulaimi
Al-Rafidain University College
Baghdad, Iraq
mohammed.khudhaer.elc@ruc.edu.iq

Aymen Mohammed Al-Dulaimi
Al-Farahidi University College
Baghdad, Iraq
aymenaldulaimi@uoalfarahidi.edu.iq

Omer Mohammed Al-Dulaimi
University Politehnica of Bucharest
Bucharest, Romania
omer_mohammed.al@stud.etti.upb.ro

Abdulqader Faris Abdulqader
Al-Noor University College
Nineveh, Iraq
abdulqader.faris@alnoor.edu.iq

Andrii Zakharzhevskyi
State University of Telecommunications
Kyiv, Ukraine
ZakharzhevskyiA@duikt.edu.ua

***Abstract* — Background: Cloud computing (CC) is a disruptive computing paradigm that uses networked systems, notably the Internet, to provide shared resources and services. Its use has been widespread, owing partly to its promise to reduce computation costs.**

Objective: This study aims to get into the critical security concerns of cloud computing and provide unique solutions to these difficulties.

Methods: By examining the operational procedures and infrastructure of data centres - the critical suppliers of cloud services - this article elaborates on the risks that cloud-based operations bring. The study underlines the need for increased security, particularly considering customers' interconnection and apparent control over ostensibly devoted resources.

Results: Cloud computing offers a variety of advantages, including on-demand service delivery, geographical independence, and pay-as-you-go pricing. However, its intrinsic structure threatens data integrity, availability, and privacy. In response, this article presents a Dynamic Secure Interconnection (DSI) architecture that divides the cloud into dynamic virtual trust zones, each with its own set of security protocols.

Conclusion: Implementing effective security measures becomes more important as cloud computing transforms IT and business environments. The suggested DSI mechanism is a viable way to bolster security inside cloud systems, aiming for a safer, more regulated data management environment.

I. Introduction

The use of cloud computing has fundamentally changed the way organisations handle their information technology and data assets. The age of stationary, locally hosted client/server systems has become obsolete, and cloud environments have evolved as more adaptable and universally accessible alternatives. This change may be illustrated in the study by Singh and Sharma, which explores security frameworks for cloud computing [1]. It has played a crucial role in decreasing the expenses associated with computing and providing solutions that can be easily expanded. Organisations expose themselves to considerable security concerns, especially regarding data protection and integrity, by transferring their data to the cloud and giving up control.

The rapid increase in the popularity of cloud computing may be ascribed to its straightforwardness and affordability. Cloud computing is a technology that provides virtualised and shared computer resources via internet-based services. The writers Qasim, Shevchenko, and Pyliavskyi emphasise the widespread use of cloud computing [2] and its positive impact on the energy efficiency of digital broadcasting. The research conducted by Md, Varadarajan, and Mandal suggests that cloud services are becoming more popular, leading to a decrease in the use of personal desktop computers and internet browsing. Instead, a growing focus is on managing data and applications on large-scale cloud networks [3].

Despite these benefits, the concentration of cloud computing makes it susceptible to specific security hazards. An inquiry conducted by Vayanaperumal, V, and R on the Enhanced Critically Self-Correlated Particle Swarm Optimisation (CSC-PSO) algorithm used in resource allocation for cloud computing demonstrates the complex and ever-changing characteristics of cloud environments, which can potentially expose sensitive data to different types of risks [4]. A further illustration of the increasing need for robust security measures in cloud systems is the study by Raji and Adam on public cloud security [5, 6]. Their inquiry focuses on user identification and the verification of data integrity.

The article introduces the Dynamic Secure Interconnection (DSI) architecture, an innovative idea that separates the cloud into dynamic virtual trust zones, each with its own distinct set of security protocols. This design is suggested as a solution to the previously identified security problems. This novel technique aims to enhance cloud security by establishing a more controlled and protected environment for data management, addressing the shortcomings of conventional cloud computing. Empirical studies have shown that the DSI technique operates as planned and has the potential to be a crucial component in future security solutions for cloud computing [7, 8].

The analysis by Hashim, Jawad, and Yu on the security implications of Long-Term Evolution (LTE) technology inside the Internet of Things provides new insights into the convergence of cloud computing and developing technologies.

The need for safe data storage and transmission is growing with the rising use of Internet of Things devices that rely on cloud computing for these functions [5, 6].

The article aims to clarify the inherent security issues in cloud computing infrastructures and provide innovative methods to improve security. Our study aims to make a substantial contribution to current efforts to improve the security of cloud computing. Our study analyses the many security risks often found in cloud settings. We also evaluate the effectiveness of current security solutions, including the DSI architecture proposed by our team. We aim to protect cloud computing environments from the ever-changing array of cyber threats using state-of-the-art security models, robust algorithms, and novel technologies.

A. Aim of the Article

The article aims to thoroughly examine and analyse the diverse security risks prevalent in cloud computing systems. Additionally, the study aims to provide viable techniques and upgrades that effectively address and mitigate these threats. Cloud computing has emerged as an essential component of contemporary information technology infrastructure, providing many advantages. However, it also poses distinctive security complexities.

This article aims to ascertain and categorise the vast array of risks cloud systems may encounter, including data breaches, illegal access, insider threats, and other related vulnerabilities. This study aims to provide cloud service providers, companies, and security experts with valuable insights into possible vulnerabilities by comprehending the landscape of these threats.

In addition, the study aims to provide suggestions for improving the security of cloud computing systems by implementing security upgrades, best practices, and recommendations. These additions may include the use of sophisticated encryption techniques, the utilisation of access control mechanisms, the deployment of threat detection systems, and the adherence to compliance frameworks. The primary objective of these measures is to safeguard the confidentiality, integrity, and availability of data and services inside the cloud environment. The primary objective of this paper is to provide a valuable contribution to the continuous endeavours in enhancing the security and resilience of cloud computing systems, particularly in response to the ever-changing landscape of cyber threats.

B. Problem Statement

The article focuses on the issue statement about the growing security problems cloud computing systems encounter. As businesses transition their data and operations to cloud environments to achieve scalability and cost-effectiveness, they are confronted with an expanding range of potential risks and vulnerabilities that pose a danger to the security of sensitive information.

Cloud computing systems are vulnerable to various security concerns, including but not limited to data breaches, illegal access, data loss, and service outages. The potential ramifications of these dangers are significant, including the compromise of user privacy, financial losses, and harm to an organisation's brand. Additionally, the security risks are further intensified by the dynamic nature of cloud environments, shared responsibility models, and complex infrastructures.

This study aims to identify, assess, and recommend security upgrades that successfully mitigate these risks. The study delves into sophisticated security methods, including encryption, multi-factor authentication, intrusion detection systems, and security information and event management (SIEM) solutions, to enhance the security stance of cloud computing platforms. The primary objective of this article is to mitigate the risks posed by various threats and establish effective security protocols to safeguard the integrity, confidentiality, and availability of data inside cloud environments.

C. Key Features of Cloud Computing Exposing

A simple, on-demand network access approach known as "cloud computing" (Fig.1) enables users to easily share computing resources, such as servers, applications, storage, and services. The following are the primary characteristics of cloud computing as described by the National Institute of Standards and Technology (NIST) [9].

On-demand self-service: Clients get on-demand access to cloud computing resources.

Broad network access: Users are no longer confined to their desks, as they can access all their files and programs via the network. Group members can be located anywhere on the planet and maintain constant contact with one another.

- Pooling of resources: The provider's computer resources are shared among numerous customers.
- Rapid elasticity: All cloud computing features can be quickly provided to customers.
- Measured service: This service's parameters can be adjusted according to the user's needs via the cloud's built-in metering mechanisms.

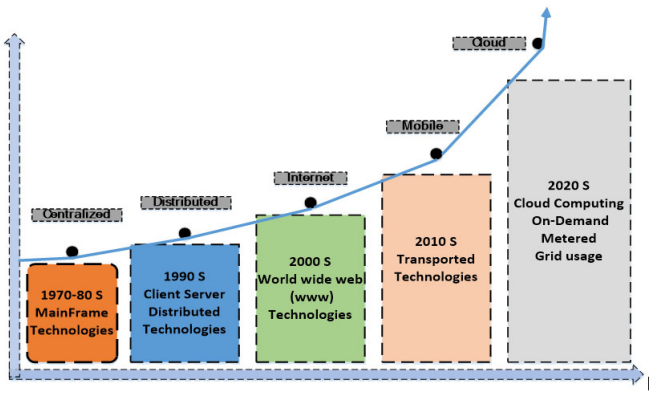

Fig. 1. Evolution of cloud computing

Cloud computing offers numerous advantages, including improved resource utilisation efficiency, on-demand service delivery, universal access, elastic resource pooling, and pay-per-use pricing. However, separating data ownership and management on virtualised platforms raises additional security

concerns [9]. To address these challenges, this study proposes a novel Dynamic Secure Interconnection (DSI) mechanism, which partitions the cloud computing system into dynamic virtual trust zones with distinct security policies for different clients. Experimental findings demonstrate the effectiveness and viability of the DSI mechanism [7, 8]. By implementing this innovative approach, cloud computing systems can bolster their security measures and ensure a more robust and protected environment for data and services.

II. Literature Review

The advent of cloud computing has brought about a significant transformation in the manner in which both enterprises and individuals procure and administer data and services. Nevertheless, the proliferation of cloud computing has led to a heightened emphasis on security problems. This literature study aims to comprehensively examine the primary security obstacles linked to cloud computing, along with the potential remedies put out in recent scholarly investigations. These sources are used to examine the dynamic nature of cloud computing security.

Access management and authentication pose significant security problems in cloud computing. Organisations and auditors with appropriate qualifications can regulate access to cloud computing services. The use of encryption is of utmost importance in guaranteeing that only authorised entities possess the capability to access unencrypted info [10]. To mitigate the

risks of data breaches and privacy violations, it is essential for access control methods to possess a high level of robustness, hence effectively preventing unauthorised access [11].

Ensuring the integrity and security of data are fundamental considerations within cloud computing. Ensuring the accuracy of information and maintaining the confidentiality of data are crucial considerations for customers using cloud storage solutions. The integrity of data may be compromised due to corrupt conduct shown by contributors, resulting in potential data loss and erosion of confidence among users of cloud services [12]. The preservation of data confidentiality in distributed systems and safeguarding it against external attacks is a substantial obstacle [11].

The present literature has several solutions for optimising resource allocation in cloud services and resource management. Nevertheless, when dealing with intricate cloud setups, the CSC-PSO algorithm exhibits remarkable performance [4]. To maintain a highly secure design, it is crucial to spread the workload throughout the cloud infrastructure fairly. This optimisation is inherently connected to security. The need to ensure secure resource allocation in protecting sensitive data inside the cloud is further emphasised by the research conducted by Adam and Raji [5], who formulated models for user authentication and data integrity.

The accessibility and availability of cloud computing are of utmost importance. The fast delivery of services is a crucial aspect of customer reliance on cloud technology. However, the availability of these services might be disrupted by natural catastrophes or system faults [10]. Maintaining the robustness of cloud infrastructure is of utmost importance to mitigate the occurrence of system unavailability and the potential loss of data. Maintaining high availability levels is contingent upon the critical aspects of network planning, scalability, and infrastructure architecture [13].

The decentralised nature of cloud computing gives rise to inquiries over the geographical placement of data and concerns regarding privacy. The storage of data on distant servers and the worldwide dispersion of service providers provide challenges in accurately determining the specific location of the cloud [10]. The factors mentioned earlier could impact adherence to data protection requirements and jurisdictional matters, necessitating meticulous oversight and openness about the locations where data is stored.

Numerous cryptographic and non-cryptographic methodologies have been suggested as potential solutions to the security obstacles encountered in cloud computing. The strategies above include measures to guarantee data availability, integrity, validity, and secrecy [10]. Encryption, secure access controls, and multi-factor authentication are identified as effective measures for enhancing access control and authentication.

In addition, using privacy-enhancing technology and establishing comprehensive confidentiality rules are crucial in safeguarding the privacy of customers' data inside cloud computing environments [11, 14]. Regularly updating and monitoring confidentiality regulations is paramount, especially in multinational clouds that transfer data across borders [15].

Mobile Cloud Computing (MCC) has significant potential within the healthcare industry since it facilitates remote health monitoring and enhances the quality of patient care. Nevertheless, the mainstream deployment of the technology has been impeded due to security concerns [13]. To fully harness the advantages of Mobile Cloud Computing (MCC) in the healthcare sector, including its portability, scalability, modernisation, efficiency, and collaborative features, it is imperative to tackle the associated security problems effectively [16].

Incorporating cloud computing has become an essential component of contemporary information technology infrastructure, presenting many benefits but concurrently presenting notable security obstacles. Ensuring the safe functioning of cloud computing systems necessitates addressing critical concerns such as access control, data integrity, availability, data placement, and privacy. Researchers have suggested numerous solutions, including encryption, access restrictions, privacy-enhancing technology, and comprehensive confidentiality rules. The healthcare industry has the potential to benefit significantly from the implementation of Mobile Cloud Computing as long as appropriate measures are taken to address security issues. The ongoing evolution of cloud computing necessitates a proactive approach to effectively resolving security problems to maintain the trust and confidence of users.

III. The composition of DSI and its elements

The study extensively examined the Dynamic Secure Interconnection (DSI) architecture as an innovative approach to bolster cloud computing security (Fig.2). This architecture

employs the shared responsibility models in cloud security, as outlined by Singh and Sharma [1], to partition the cloud into distinct "trusted zones" with tailored security rules. The design of DSI requires many crucial components.

1. Trusted Zone Creation: DSI is establishing "trusted zones" inside virtual clouds, building upon the research conducted by Qasim, Shevchenko, and Pyliavskyi [2] on energy-efficient digital broadcasting. These zones are delineated based on their security protocols and requirements, which are contingent upon the level of confidentiality of the data housed inside them.

2. Dynamic Interconnection Mechanism: Data flow management is entrusted to a dynamic system that considers real-time risk assessments and predefined security protocols. This method is used to consolidate these regions. The complexity of cloud formations is seen in the tests conducted by Vayanaperumal, V, and R [4].

3. Security Protocol Layers: By the approach used by Raji and Adam in developing their frameworks for user authentication and data integrity [5], each DSI zone is equipped with a distinct collection of security protocols, including intrusion detection systems and encryption, which are essential for its operation.

4. Monitoring and Management Module: The DSI architecture is managed by a centralised monitoring system that ensures security analysis and prompt threat detection, similar to Mahmoud's [12] concept of cloud-based management systems.

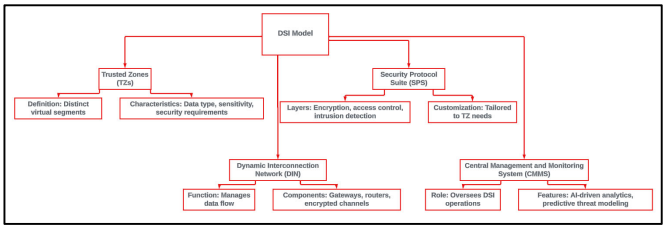

Fig. 2. Dynamic Secure Interconnection Model Components

The concept of DSI involves partitioning the resources of the cloud into distinct secure zones, which are tailored to meet the specific security needs of individual users (Fig.3). Following the data security frameworks proposed by Bai et al.[13] Moreover, Latha and Sheela [14], areas responsible for managing sensitive data enforce stricter security measures than areas that handle less sensitive data.

We are analysing a specific instance of an application hosted in the cloud in a healthcare environment.

Envision a hypothetical healthcare cloud system that employs the DSI paradigm, akin to the security enhancements elucidated by Shabbir et al.[16] in mobile cloud computing.

The Patient Records Zone is fortified with stringent access controls and robust encryption protocols to protect vital patient data. The privacy-preserving solutions for cloud computing provided by Zou et al. [17] are adhered to.

The Research Data Zone emphasises the importance of data integrity and accessibility for scientists. It incorporates components from the advanced bacterial foraging optimisation algorithm proposed by Anand, Varadarajan, and Anand [11] to ensure secure data storage.

The Administrative Information Zone corresponds to the efficient and accessible intelligent monitoring techniques for IaaS clouds proposed by Prasad and Bhavsar [18].

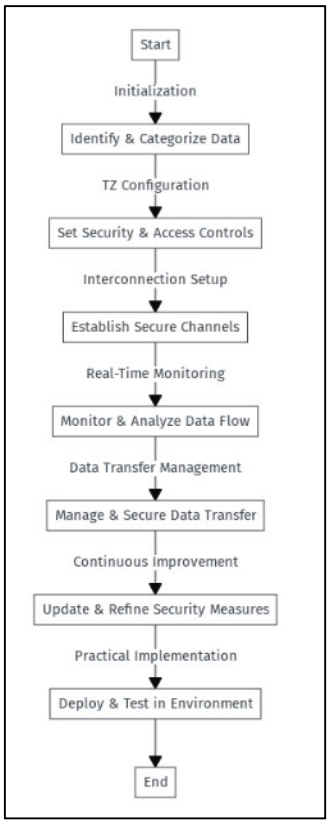

Fig. 3. Dynamic Secure Interconnection Algorithm

This case study demonstrates DSI's capability to comply with healthcare laws and guarantee data security via secure zone-to-zone transfers. The concept's practical usefulness aligns with recent cloud computing security research advancements. The adaptability of this technology enables the modification of security protocols to counter emerging and evolving threats effectively.

IV. The Role of CSC-PSO in Resource Allocation

The Critically Self-Correlated Particle Swarm Optimisation (CSC-PSO) algorithm, developed by R, Vayanaperumal, and P [4], is a unique method in cloud computing that focuses on optimising resource allocation, a crucial part of cloud security. A reflecting mechanism is established by including a self-correlation component in the traditional Particle Swarm Optimisation framework. This mechanism allows particles (possible solutions) to evaluate their future path by considering their prior performance and the collective intelligence of the swarm. Robust security requirements are essential in cloud computing, requiring careful allocation of resources and highlighting the need for strategic self-analysis. Optimal resource allocation is essential for load balancing in cloud

architecture (Fig.4) to mitigate security risks caused by insufficient or excessive resources. The compatibility of CSC-PSO with the shared responsibility models in cloud security, as outlined by Singh and Sharma [1], which highlights the need for dynamic resource management to ensure the reliability of cloud services, increases its effectiveness in this field. Md, A.Q., Varadarajan, and Mandal [3] and Raji and Adam [5] address interconnected topics; the former highlights the need to effectively identify in cloud networks, while the latter concentrates on constructing models for user authentication and data integrity. In their research, Gai et al. [10] investigated the impact of CSC-PSO on cloud security. They concluded that it can significantly improve emerging security models that include blockchain and other evolving technologies. This presents favourable opportunities for safeguarding cloud infrastructure in the cyber domain.

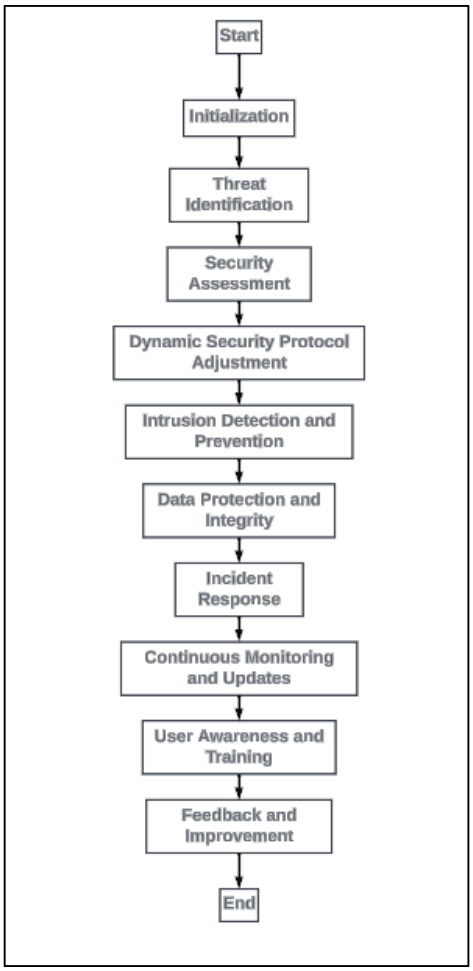

Fig. 4. SecureCloud Algorithm: Proactive Threat Management in Cloud Computing

V. METHODOLOGY

According to the delivery models, there are three categories for cloud computing, including infrastructure as a service (IaaS)[19], as shown in Figure 5.

IT resources, including data storage, networks, and processing power, are available as a service. In the cloud, customers can rent server time, working memory, data storage, and the ability to run their operating systems and applications [17].

This sort of software uses a distributed model and contains all programs kept on the service provider's servers and makes them accessible to cloud customers online. The SaaS is well-liked and used more frequently because it supports web services. Pay-as-you-go subscription licensing is also connected to SaaS. Web browser security is crucial since applications are accessed through them over the Internet [17]. There are several ways to secure SaaS services using encryption, all of which are considered extremely important. To enforce data protection when it is transmitted over the Internet, a Secure Socket layer (SSL) and other options are utilised [20].

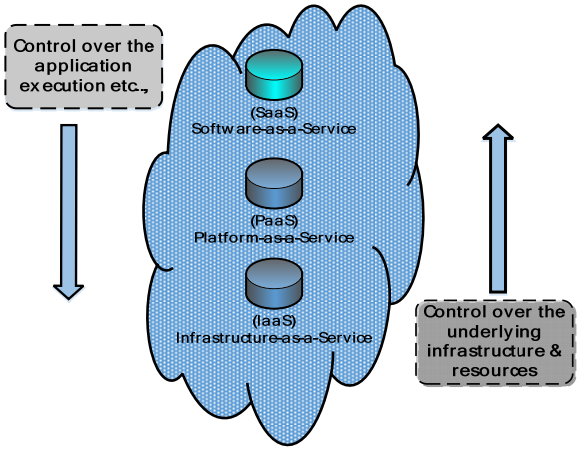

Fig. 5. Categories of Cloud Computing

Platform as a Service (PaaS): The PaaS provider offers standardised interfaces to the client's services. The platform as a service offers multi-tenancy, access control, and database access. Customers can use the platform to run their programs, but they do not have access to the hardware or operating system [21, 22]

A. Types of cloud computing

There are four basic types of clouds, and each is distinguished by its infrastructure's location, availability, and control access—all of which affect the type employed [23].

Public Cloud: The cloud infrastructure is operated and managed by a third party or the organisation solely for that organisation. It might be present on-site or elsewhere. The key benefits are management overhead and cost-effectiveness in capital expenditures. The drawbacks include privacy performance, latency, and security issues [24, 25].

Private Cloud: This type is based on internal or external resources and has more control over corporate data. Purchasing or operating infrastructure to enable the cloud has a higher cost. The third party or the organisation manages and operates the cloud infrastructure exclusively on behalf of the enterprise. It might be present on-site or elsewhere. The managerial overhead and expense are the key benefits.

Community Cloud: This kind of cloud benefits from both the public cloud's economic advantages and its high level of security. Numerous firms utilise it with comparable security requirements and need to store or process sensitive data [24].

Hybrid Cloud: This cloud connects a private cloud to other third-party cloud services. It offers an IT solution by fusing the private and public clouds. More security measures are in place for both data and apps. This cloud enables external parties to access information online and has more secure data and applications. Interfaces with other management systems are also possible [26].

B. The security threats of cloud computing

1) Abuse and criminal use of cloud computing

In this attack, unauthorised individuals can enter a public cloud and Fig. out how to upload spam and malware to numerous computers while exploiting the cloud's infrastructure to target other devices. The following suggested countermeasures are used to prevent these attacks [27]:

- Verify the authenticity of the initial registration procedure.
- Increase credit card fraud detection efforts.
- In-depth analysis of the client's system infrastructure.
- Insecure application programming interfaces (APIs).

2) All users access the cloud through interfaces.

These interfaces must use exceptionally secure authentication, access control, encryption, and monitoring approaches. The suggested remedial techniques are:

- The interfaces of the providers' security models need to be examined.
- Strong authentication and access control must be employed.
- Encryption has to be applied during transmission [20, 21].

3) Malicious Insiders threats

Many service providers need to be mindful of who they hire and who they give access to the assets. It is crucial to keep an eye on them to prevent malicious behaviour and threads; to address such issues, the following steps must be taken [20, 28]:-

- Legal agreements must cover all of an employee's resources.
- Implement chain management and carry out supplier evaluation
- It is essential to think about security breach notifications.

4) Vulnerabilities of Sharing Technology

Employing the infrastructure as a service (IaaS) cloud computing is standard practice. However, the infrastructure's components are not made for that. Therefore, monitoring and compartmentalisation are needed to ensure clients do not pose a hazard to one another on their property. The following actions need to be taken to decrease the threats [29]:

- Illegals' actions need to be watched closely.
- Secure setup and configuration.
- Scanning for vulnerabilities is recommended.

5) Data loss

Data must be secured from loss because customers need to use it. Unauthorised access could result in the theft of data. The data is in danger if deleted without a backup or if the encryption key is lost. Data security is a significant problem that must be protected by law and the business's reputation. The following actions must be followed in order to prevent these threats [30]:

- We are using encryption to safeguard data.
- Employing strict access control measures
- Retention policy determination.

6) Service, account, and traffic hijacking

There are other threats that cloud users should be aware of. Denial of service is one of these possible threats [22, 31]. To keep away from them. The subsequent actions are taken:

- Sharing must be outlawed amongst users.
- Use robust authentication methods.
- The provider must have strict security.

C. Failure of the provider's security

A provider's security failure occurs when a cloud service provider's security procedures are hacked or breached, resulting in possible vulnerabilities and hazards for the data and resources in the cloud. While cloud computing has many advantages, such as rapid access to computer resources, scalability, and cost-effectiveness, it also exposes users to security risks [32].

Unauthorised access to confidential information, data theft, information loss, or service outages may occur when a provider's security procedures fail. Hackers or malicious individuals may exploit flaws in the provider's software, hardware, or settings to get unauthorised access and valuable information.

To reduce the dangers associated with a service provider's security [33] failure, cloud customers must establish strong security practices such as tight access restrictions, encryption, frequent monitoring, and assuring that they comply with industrial security standards. Furthermore, customers should choose known and trustworthy cloud service providers that prioritise security and have a track record of adopting appropriate security measures.

Frequent security audits and upgrades are essential for quickly discovering and fixing possible issues. Cloud customers may considerably lower the probability of becoming victims of a provider's security breach and improve the general safety of their information and activities in the cloud by adopting proactive steps and being attentive.

D. Attacks by other customer's number

Multi-tenancy attacks, also known as assaults using other customers' numbers, are security concerns arising in cloud computing infrastructures where several clients or users share the same basic infrastructure and services. In this scenario, one customer's activities or vulnerabilities may influence the safety and efficiency of other clients hosted on the same cloud platform.

Multi-tenancy is a crucial feature of cloud computing that allows for cost savings and resource optimisation by sharing computer resources among users [7]. This shared environment, however, raises security issues. One of the most severe worries is that a malevolent user may exploit weaknesses in the cloud infrastructure to get unauthorised access to other customers' data or interrupt their services.

Among the most prevalent assaults by other customers' numbers are:

- Cross-Tenancy Data Breach: A malevolent client may acquire unauthorised access to other customers' data and resources if a cloud provider fails to provide adequate isolation procedures. This sort of assault might expose sensitive information, which can have severe ramifications for targeted organisations.
- Exhaustion of Computing Resources: An aggressive or compromised client may purposefully utilise excessive computing resources, resulting in denial-of-service (DoS) issues for other tenants using the same resources.
- VM Escape: A hostile customer may break out of their assigned VM and obtain access to the hypervisor or underlying infrastructure to compromise other VMs on the same host.
- Side-Channel Attacks: Attackers may harvest sensitive information from neighbouring virtual instances by exploiting common resource features such as cache latency or memory access patterns.

Cloud service providers use security measures [30] such as tight isolation, virtual network segmentation, access restrictions, and monitoring to reduce the danger of multi-tenancy attacks. Customers must also adopt best practices when safeguarding their apps and data in the cloud.

Regular security audits, patch management, and threat monitoring are required to discover and remedy vulnerabilities quickly. Educating users on the hazards of cloud security and maintaining compliance with security standards are also critical elements in developing a safer multi-tenant cloud infrastructure.

E. Availability and Reliability Issues

In cloud computing, availability and dependability are vital considerations since they directly affect the ongoing availability and efficiency of services supplied to consumers. To satisfy consumer requests and retain their market reputation, cloud service providers must guarantee that their systems are highly available and dependable [34].

One of the most challenging aspects of assuring availability is minimising downtime. Any service disruption might result in considerable financial losses for firms that depend on cloud services. Various factors, including hardware problems, network outages, and software defects, may cause downtime. TCloud providers invest in redundancy and failover measures to lessen the effect of such failures; they often install data centres in various geographic locations, allowing data and services to be duplicated across numerous sites, assuring continued availability even if a regional failure occurs.

The consistency and predictability of cloud services are referred to as reliability. Users anticipate that their apps and data will always be available and reliable. High dependability requires extensive testing, quality assurance, and continual cloud infrastructure and services monitoring. Furthermore, frequent updates and patches are required to address any vulnerabilities that may jeopardise dependability [35].

SLAs (Service Level Agreements) are critical in specifying cloud services' anticipated availability and dependability. These agreements detail the performance measurements and uptime guarantees provided by cloud providers. They also

establish consequences for failing to reach agreed-upon service standards, motivating providers to maintain high availability and dependability [18].

F. Integrating customer and supplier security systems

Linking client and vendor security systems is critical for ensuring a safe and trustworthy environment in cloud computing. Cloud service suppliers and their clients must collaborate to maintain the security of data and resources.

By integrating security solutions, customers may get greater visibility and control over their data and apps in the cloud. They may put security measures and procedures in place to protect sensitive data and prevent unauthorised access. Simultaneously, cloud providers may adapt their security policies to client needs, delivering a standardised and comprehensive security architecture [36].

Customers and cloud providers must communicate and share information in real-time for integration to be effective. This involves receiving frequent security updates, coordinating incident response, and monitoring possible threats in real-time. In order to simplify security management and response, clear roles and duties should be identified [37].

Integrating customer and supplier security systems increases confidence and transparency among all stakeholders.

It improves the cloud environment's overall security posture and reduces the risks related to information breaches and cyberattacks.

The potential use of blockchain technology in strengthening the security of cloud services is now being investigated. This topic has seen substantial advancement in recent years. According to the study by K. Anand, A.V., and M. Vijay Anand [11], blockchain technology can significantly improve privacy protection and ensure safe data storage. Furthermore, using essential management methods in data privacy and security frameworks is advantageous due to the decentralised nature of blockchain technology, which enhances cloud security. This assertion is confirmed by Shafi, Y.K.a.M. [21].

VI. Results

Identification: The identification is based on the delivery model and cloud type. Individual cloud user names (IDs) and passwords are validated to safeguard each user's cloud profile. This results in the security of cloud profiles **Ошибка! Источник ссылки не найден.**.

Authentication: It also relies on the kind of cloud and the delivery model. The users must first be identified before allocating access priorities and permissions. The authentication process is then done by verifying IDs and passwords **Ошибка! Источник ссылки не найден.**.

Confidentiality: Maintaining control over an organisation's data, which is spread across various distributed databases, is the core task of cloud computing.

Authorisation: Maintaining integrity is one of the critical information security needs for cloud computing. In private cloud computing, the system administrator keeps track of the authorisation **Ошибка! Источник ссылки не найден.**.

Anonymity means that the system software or the node itself should not distribute the information used to identify the present user or the owner of an anode.

Integrity: One prerequisite for cloud computing is integrity, which ensures the isolation, consistency, and durability of access to data within the cloud domain.

Non-repudiation: This can be attained by implementing e-commerce security protocols, such as time stamps and digital signatures, to the data transmission within cloud applications.

Availability: It is among the most crucial cloud computing information security criteria. It is the primary variable in choosing a specific form of cloud computing (public, private, and Hybrid clouds) (Fig.6).

As a result of exploring the information security requirements across different cloud deployment and delivery models, the organisation and the vendor have gained increased confidence in promoting a secure cloud framework.

Privacy: It is a crucial issue for cloud computing and must be considered at every stage of the design process **Ошибка! Источник ссылки не найден.**. For those designing cloud systems, the following advice has to be considered:

A minimum amount of personal data must be saved in the cloud.

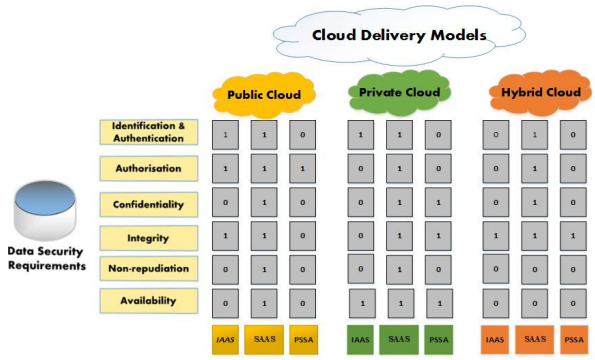

Fig. 6. Cloud computing for security

- Guard personal data stored in the cloud.
- Define and restrict the storage of data's purpose.
- Increase user control.

Identify and Access Management: A good unified authentication infrastructure and strategy are required for a firm to handle IDs at cloud providers.

Security governance: The security steering committee must outline the duties and processes for the safety team and other organisations performing security activities **Ошибка! Источник ссылки не найден.**.

A. Network security

Cloud computing faced many security problems in the past. These problems came due to the misuse by placing malware there or using their processing power to crack the passwords. To prevent these attacks, the Cloud Security Provider should take the necessary precautions to protect the network. Some attacks like Trojan horses, viruses, spam, and covered channels can be prevented using anti-virus programs or firewalls. Encryption is used for interactions between CSP and clients and between the provider's sites to function securely and prevent assaults. If a third-party supplier is necessary to supply the services, contact with them must likewise be encrypted. **Ошибка! Источник ссылки не найден.**. As long as the resources are concentrated in the data centres, the main attack for DDoS attacks on publicly traded cloud computing networks has a bit rate of more than 10 Gbps. Many CSPs can hardly defend against DDoS attacks. Each public CSP should take proper measures against this type of attack by using high data rates, and this option can be obtained and bought. Major internet service providers (ISPs) provide these mitigation services, and agreements govern their usage. Internal DDoS attacks must be avoided by taking the necessary precautions. Cloud customers may perpetrate that. Since cloud computing plate forms consist of many components, the system's configuration must be well organised; otherwise, many successful attacks can be perpetrated on the system **Ошибка! Источник ссылки не найден.**.

B. Information Protection

Data production, storage, dissemination, consumption, and destruction are all parts of the data life cycle. Cloud Service

Providers (CSPs) are essential in installing proper security features to assist these stages. All clients share shared data storage in the context of various kinds of memory storage technologies, demanding safe separation of their data to provide confidentiality and prevent unauthorised access.

Web-based applications must be securely developed to prevent SQL injection and other unauthorised data access techniques to protect against possible vulnerabilities. Strong security measures are critical to protecting consumer data from unauthorised tampering or destruction. As part of the data security strategy, regular data backups are performed to ensure data integrity and recoverability in the event of technological failures, parameterisation difficulties, or media obsolescence.

CSPs must evaluate the usefulness of data backups regularly to ensure they can be reinstalled appropriately when required. In the case of a backup problem, CSPs must quickly notify customers and offer openness and transparency of the backup information.

CSPs are responsible for thoroughly and reliably erasing all consumers' data from current and prior storage media at the end of a contractual relationship. To guarantee data privacy and adherence to rules, ensure data deletion is done safely and irreversibly.

Finally, CSPs rigorously manage the data life cycle, emphasising the necessity of security measures, data backups, and extensive data deletion procedures to preserve client data confidentiality, integrity, and availability throughout its lifespan inside cloud environments.

C. Data Security Model

Validation Process:

Level 1 Validation is the initial checkpoint where incoming data is authenticated. It involves checking the integrity and authenticity of the data against predefined security protocols—Utilises SHA-256 for data integrity checks.

Cryptography/Encryption: Once the data passes Level 1, it undergoes encryption. Encryption at this stage ensures that even if the data is intercepted, it cannot be understood without the correct decryption key. Employs AES-256 for data encryption.

Level 2 Private Security: After encryption, the data is subjected to another layer of security checks within the private security domain to further validate and protect against internal threats. Features IDS and AI-based anomaly detection.

Level 3 Fast Recovery: In the event of a security breach or data loss, the system has a mechanism to recover the data quickly. This may involve backup systems or redundant data storage. Incorporates real-time data replication and RAID systems.

Encryption and Validation Process:

Distributed Matrix (Df): The distribution matrix represents how data is spread across multiple nodes in the cloud

$$D_f = C(Node\ Name)$$

signifies the assignment of file fragments to different nodes.

Data Distribution State (Kf): This represents the state of data after it has been distributed across nodes.

$$K_f = f \times D_f$$

defines the relationship between the files and their distribution matrix.

Encryption Process (Ef): The encryption process is block by block, transforming the file into an encrypted vector. $E_{(f)}$ represents the encryption of file f into blocks.

File Representation (f): A file f can be described as a set of blocks $F(1), F(2), F(3), \cdots F(N)$.

Distributed Matrix Representation (Df matrix): This is an $L \times L$ matrix, where L is the number of data nodes.

Enhanced Encryption Process:

Private Protection Model (D'f): Represents the protected model of the distributed message.

$$D'f = CA\ (Node\ Name)$$

Where CA denotes an authentic visit to the node name.

Resolution of the Private Matrix (M): M resolves the private matrix into a format suitable for encryption.

Encrypted File Vector (Kf):

$$Kf = E_{(f)} \times D_f$$

provides the state of the encrypted file distributed across the nodes.

The model can be shown in Fig. 7.

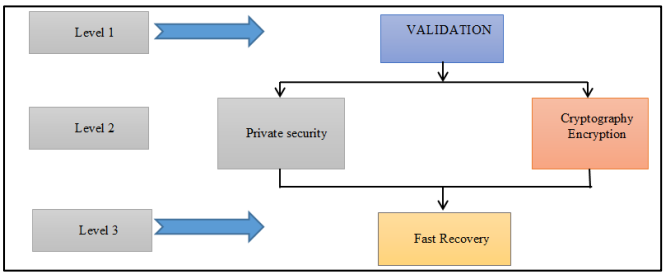

Fig. 7. Data Security Model

The model for security cloud computing consists of 3 levels of defence: The first layer is used for the authentication of customers and management of data operations (Add, modify, delete) performed at this level. Any vulnerability in the user authentication system will permit unauthorised users to access the system. The data is encrypted in this layer; even if the key was illegally accessed, the intruder cannot access the adequate information because encryption and privacy support this level against attacks.

Suitable Encryption method is used to transfer sensitive data secretly. They are looking for appropriate critical management methods to handle the encryption method. The customer can cypher the data before storing them; in this case, they must handle all the critical management themselves. If the provider encrypts the data, security measures have to be considered

regarding the used, shared, stored, and destroyed data, which should be based on confidentiality, integrity, and authenticity. The providers should inform the customers of the cryptographic mechanic (i.e. linear feedback shift register encryption or other methods) used. The critical management should consider the following instructions:

- Select key generators to form keys in a secure environment.
- The distributed keys should be done securely.
- The cryptographic keys should have a dedicated purpose only.
- Keys should not be stored in clear form but always encrypted, and the storage should redundantly back up.
- The keys should be changed regularly.
- Separate authentication should be made to the critical management functions.
- All keys that have expired must be destroyed in a secure manner.
- The archive of keys should always be in safe mode.
- Critical
- management requires adequate cryptographic skills, and the cloud service provider (CSP) personnel should have good knowledge and training in the cryptographic field.

VII. Discussion

The article examines the crucial topic of cloud computing security risks and investigates several techniques for improve cloud-based systems' safety. Cloud computing has transformed the IT sector by enabling flexible and cost-effective data storage, processing, and delivery of services. However, the intrinsic structure of cloud computing, in which information and assets are shared among several users and housed on distant servers, creates some security issues.

Given the shared responsibility approach, the article emphasises the significance of a robust security architecture for cloud computing [1]. This approach emphasises cooperation between cloud service providers and clients to maintain a safe environment. It explicitly describes each party's tasks and obligations regarding security measures such as data protection, access limits, and threat mitigation.

One of the primary dangers mentioned in the article is connected to cloud computing resource allocation. Resource allocation efficiency is critical for optimising cloud performance and satisfying user needs [4]. Improper resource allocation may result in resource waste or overutilisation, exposing the cloud infrastructure to security breaches. The authors present an improved critically self-correlated particle swarm optimisation (CSC-PSO) resource allocation method to improve overall cloud security.

Energy efficiency is another component of cloud security mentioned in the article. Energy consumption is a significant issue in large-scale cloud data centres [6]. The article examines numerous approaches for increasing the energy efficiency of digital broadcasting in cloud-based systems, which may aid in lowering operating costs and environmental effects.

The article recommends using secure data storage and user authentication procedures to improve the security of cloud services [3, 5]. These safeguards are critical for safeguarding sensitive data and preventing unauthorised access to cloud resources. The authors offer models and methods for safe data storage and user authentication

to improve public cloud security.

Combining cloud computing with emerging technologies such as the Internet of Things (IoT) raises new security concerns [6]. The article examines the current status and future possibilities of Long-Term Evolution (LTE) technology in the Internet of Things, emphasising the need for secure communication and data sharing between IoT devices and cloud-based systems.

The report on cloud computing security problems [9] shows a variety of dangers, such as data breaches, insider assaults, and Denial-of-Service (DoS) attacks, among others. Understanding these dangers is critical for developing effective security solutions to protect cloud systems.

The article investigates the role of blockchain technology in improving cloud computing security [10]. Blockchain technology's decentralised and tamper-resistant features offer a secure foundation for data exchange and transaction verification in cloud settings.

Another vital issue covered in the article is cloud forensics, which focuses on improving the structure of cyber threats in cloud settings [38]. This entails researching and analysing security occurrences to collect evidence for probable cyberattacks or breaches.

The article sheds light on the varied nature of cloud computing security risks and the necessity for comprehensive security solutions. The article adds to current efforts to improve cloud security and ensure the safe and dependable functioning of cloud-based systems by analysing several research publications, suggesting new algorithms, and examining the integration of multiple technologies.

VIII. Conclusion

The article has highlighted the significant effects of cloud computing, which provides flexible and scalable services globally, while also recognising the security threats that cause concerns in the digital realm. The article highlights the crucial importance of the Dynamic Secure Interconnection (DSI) model. This modern technology may improve the security, integrity, and accessibility of cloud-based data and services to provide vital protection.

Based on the shared responsibility paradigm, the DSI model is a crucial framework that encourages attentive cooperation between cloud service providers and their clients. Collaboration is not only suggested but also obligatory in the proposed coordinated effort to adopt complete security measures described in this model. To ensure cloud infrastructure protection, we have introduced resource optimisation using the innovative Critically Self-Correlated Particle Swarm optimisation (CSC-PSO) technique. The CSC-PSO's smart

resource allocation showcases its capacity to optimise the security infrastructure and prevent possible hazards.

Furthermore, the discussion has highlighted the excessive energy use of data centres, thereby emphasising the need for energy efficiency as a significant obstacle. Efforts have been made to research techniques for improving energy efficiency in cloud-based digital broadcasting to reduce costs and protect the environment.

The report highlights that secure data storage and effective user authentication systems are the two main requirements for protecting sensitive information from unauthorised access. The need to ensure secure transmission and communication channels becomes more significant as cloud computing and the Internet of Things merge. These are crucial for maintaining data integrity inside IoT systems.

Moreover, the potential use of blockchain technology presents encouraging opportunities to advance cloud security. Thanks to its unchangeable ledger, it brings about a significant change towards safe data transfers and verification of transactions, leading to a new age of cloud ecosystems resistant to tampering.

Cloud forensics is becoming more critical in investigating cyber threats since it allows for examining and understanding the underlying processes involved in security breaches. This insightful investigation is essential to comprehend fully the complex cyber dangers that affect cloud systems.

This article is a valuable resource for up-to-date research and advanced algorithms. It may also be used to incorporate various technologies into cloud security. To prioritise the safety of service providers and end users, we consistently research to improve the security of cloud systems via joint efforts. It is crucial to consistently include security considerations in plans for cloud computing since they are essential for the continued effectiveness of cloud-based solutions in our more digitalised world. Cloud security has progressed from a mere desire to a concrete and achievable reality. The DSI model and CSC-PSO algorithm provide ongoing support for this consistent advancement.

REFERENCES

[1] U. Singh and A. Sharma, Cloud computing security framework based on shared responsibility models. Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0, 2021: p. 39-55.

[2] Qasim, N., Y.P. Shevchenko, and V. Pyliavskyi, Analysis of methods to improve energy efficiency of digital broadcasting. Telecommunications and Radio Engineering, 2019. 78(16).

[3] Md, A.Q., V. Varadarajan, and K. Mandal, Efficient Algorithm for Identification and Cache Based Discovery of Cloud Services. Mob. Netw. Appl., 2019. 24(4): p. 1181–1197.

[4] R, G., R. Vayanaperumal, and P. v, An Enhanced Critically Self Correlated Particle Swarm Optimisation (CSC-PSO) algorithm for efficient Resource Allocation in Cloud Computing. 2022.

[5] Raji, A. and M. Adam. Enhancing Public Cloud Security by Developing a Model for User Authentication and Data Integrity Checking. 2020.

[6] Hashim, Q.N., A.-A.A.M. Jawad, and K. Yu, Analysis of the state and prospects of LTE technology in introducing the Internet of Things. Norwegian Journal of Development of the International Science, 2022(84): p. 47-51.

[7] F. Imran, Y.Y., and M. Ikram, Cloud Computing Security Issues And Threats In Business Environment. GSJ, 2019. 7(7).

[8] Jawad, A.M., et al., Near field WPT charging a smart device based on IoT applications. TTSIIT, 2022: p. 12.

[9] Amalarethinam, G., S. Edel, and E. Rajakumari, A Survey on Security Challenges in Cloud Computing. 2019: p. 133-141.

[10] Gai, K., et al., Blockchain Meets Cloud Computing: A Survey. IEEE Communications Surveys & Tutorials, 2020. 22: p. 2009-2030.

[11] K. Anand, A.V., and M. Vijay Anand, An enhanced bacterial foraging optimisation algorithm for secure data storage and privacy-preserving in the cloud. Peer-to-Peer Netw. Appl, 2022: p. 1-14.

[12] Mahmoud, M., Cloud-Based Control Systems: Basics and Beyond. Journal of Physics: Conference Series, 2019. 1334: p. 012006.

[13] Bai, J., et al., Virtual-Blind-Road Following-Based Wearable Navigation Device for Blind People. IEEE Transactions on Consumer Electronics, 2018. 64(1): p. 136-143.

[14] Latha, K. and T. Sheela, Block-based data security and data distribution on multi-cloud environment. Journal of Ambient Intelligence and Humanized Computing, 2019.

[15] Infante, A., J.C. Infante Moro, and J. Gallardo Pérez, Key factors in implementing Cloud Computing as a service and communication tool in universities. 2020. 631-636.

[16] Shabbir, M. et al., Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing. IEEE Access, 2021. PP: p. 1-1.

[17] Zou, Y., et al., Highly Secure Privacy-Preserving Outsourced k-Means Clustering under Multiple Keys in Cloud Computing. Security and Communication Networks, 2020. 2020: p. 1238505.

[18] Prasad, V. and M. Bhavsar, Preserving SLA Parameters for Trusted IaaS Cloud: An Intelligent Monitoring Approach. Recent Patents on Engineering, 2019. 13.

[19] Yurii Khlaponin, O.I., Nameer Hashim Qasim, Hanna Krasovska, Kateryna Krasovska. Management Risks of Dependence on Key Employees: Identification of Personnel. 2021. CPITS.

[20] V. Kumar, A.A.L., S. Karim, M. Shakir, and A. A. Brohi, Comparison of fog computing & cloud computing. Int. J. Math. Sci. Comput, 2019. 1: p. 31–41.

[21] Shafi, Y.K.a.M., A model-driven platform for service security and framework for data security and privacy using key management in cloud computing Int. Res. J. Eng. Technol, 2019. 10(6): p. 1464–1471.

[22] Nameer Hashim Qasim, A.M.J.A.-A., Haidar Mahmood Jawad, Yurii Khlaponin, Oleksandr Nikitchyn, Devising a traffic control method for unmanned aerial vehicles with the use of GNB-IoT in 5G. Eastern-European Journal of Enterprise Technologies, 2022. 117(9): p. 53-59.

[23] I. Rasheed, L.Z., and F. Hu, A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing. Comput. Networks, 2020. 176.

[24] Murugaboopathi, U.U.a.G., Enhanced security using hybrid parallel integrity key data service access control method in virtual cloud. J. Green Eng, 2020. 10(2): p. 342–359.

[25] S.V. Tyutsyura, E.V.W., Methods of projecting object models onto data structures Management of the development of complex systems, 2014. 20: p. 92-98.

[26] Hashim, N., et al., New approach to the construction of multimedia test signals. International Journal of Advanced Trends in Computer Science and Engineering, 2019. 8(6): p. 3423-3429.

[27] F. K. Parast, C.S., S. Nikam, H. I. Yekta, K. B. Kent, and S. Hakak, Cloud computing security: A survey of service-based models. Comput. Secur., 2022. 114.

[28] Qasim, N. and V. Pyliavskyi, Color temperature line: forward and inverse transformation. Semiconductor physics, quantum electronics and optoelectronics, 2020. 23: p. 75-80.

[29] Srivastava, P. and R. Khan, A Review Paper on Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 2018. 8: p. 17.

[30] C. H. S. S. Prasad, B.P.Y., S. Mohmmad, M. Gopal, and K. Mahender, Study of threats associated with cloud infrastructure systems. IOP Conference Series: Materials Science and Engineering, 2020. 981(2).

[31] Zhang, K., et al., A new method for traffic forecasting in urban wireless communication network. EURASIP Journal on Wireless Communications and Networking, 2019. 2019.

[32] Sun, H. and X. Wang, High-dimensional feature selection in competing risks modelling: A stable approach using a split-and-merge ensemble algorithm. Biometrical Journal, 2023. 65(2): p. 2100164.

[33] Khlaponin Yu.I., K.L.M., Kozubtsov I.M., Shtonda R.M., Functions of the information protection system and cybersecurity of Critical Information Infrastructure. Cybersecurity Education, Science,

Technology, 2022. 3(15): p. 124-134.
[34] Yang, M., et al., The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain. IEEE Access, 2022. 10: p. 68618-68632.
[35] Natalino, C., A. Rostami, and P. Monti. Storage Protection with Connectivity and Processing Restoration for Survivable Cloud Services. in 2021 International Conference on Computer Communications and Networks (ICCCN). 2021.
[36] Aldallal, A. and F. Alisa, Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning. Symmetry, 2021. 13(12): p. 2306.
[37] Sauber, A.M., et al., A New Secure Model for Data Protection over Cloud Computing. Computational Intelligence and Neuroscience, 2021. 2021: p. 8113253.
[38] Sudha, V.S.B.a.T., Enhancing the Structure of Cyber Risks in Cloud Environment Using Cloud Forensics Technique. Proceedings of the 2nd International Conference on Computational and BioEngineering, 2021: p. 251–257.