International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Protecting Data in the Cloud Using an Efficient Evolutionary Algorithm and a Non-Commutative Encryption Method

Dr. Jaikumar M. Patil[1], Prof. Shubhangi Y. Chaware[2], T. R. Harinkhede[3], Prof. Devendra B. Dandekar[4], Dr. Arvind R. Bhagat Patil[5], Dr. Amit N. Thakare[6]

Submitted: 19/01/2024 **Revised**: 28/02/2024 **Accepted**: 05/03/2024

Abstract: Cloud computing refers to an architectural concept that allows users to dynamically access any kind of service over the Internet on an as-needed basis, as well as supply computer and storage capacity as a service. Storage as a service is a particularly noteworthy service that is being offered. As virtualization technology evolves, datacenters often encounter the difficulty of handling a high volume of requests for virtual machines (VMs). The sheer volume of server requests has made exhaustively searching for the optimal server location to achieve certain design goals an impractical task. Datacenter administrators have so turned to heuristic optimisation techniques to determine where to put servers. The study presents a solution to the virtual machine placement issue in datacenters by combining the wake-sleep algorithm with a Cuckoo search (CSO) method. In order to do this, the suggested framework establishes a system of information security. Here, the optimal server selection procedure is carried out by the Cloud Service Provider (CSP) using the wake-sleep algorithm in conjunction with a cuckoo search. Following the selection of the server, the client employs homomorphic encryption to secure their data. By applying computations to cipher text, one may produce an encrypted result that, when decoded, corresponds to the outcome of operations carried out on the plaintext; this kind of encryption is known as homomorphic encryption.

Keywords: *Cloud computing, virtual machine (VM), Cloud Service Provider (CSP), Cuckoo search (CSO) algorithm*

1. Introduction

Over the last decade, cloud computing has emerged as a robust computing platform, offering many benefits to service providers and their customers alike. Customers may take use of cutting-edge technology and affordable processing power by outsourcing their difficult calculations, which is one of the clear major benefits. An important justification for the widespread adoption of cloud computing in several sectors is the relative cost-effectiveness of cloud technology [1][2]. Many firms have shown their preparedness to use the cloud and reap its benefits in recent years, and a corporate culture that embraces cloud computing has emerged. However, corporations are increasingly discovering that there are many security concerns that must be addressed when stepping into the cloud[3]. One of the most critical concerns in security is the privacy of sensitive data. Some data may inflict significant harm to those who control it if it were to leak. It is recommended that we encrypt our data before putting it on a distant cloud server in order to preserve its privacy[4]. Customers may protect their data while sending it to the cloud by using traditional encryption methods like RSA, AES, or 3DES. However, if they want their data to undergo more complicated processing in the cloud, they will need to exchange their private key with the server. When thinking about the cloud as an untrusted domain, the conventional usage of encryption may not be the most secure option[5]. The Cloud user may be certain that their data will be kept secure, intact, and available by modifying a few processes to lessen the likelihood of security breaches. Cloud computing and the problems with its security have been identified and addressed in this paper. Next, we went over the difficulties associated with using classical encryption as a countermeasure against threats. The concept of cloud computing came from the fast expansion of online communication and the availability of technology. Using the internet, or the "Cloud," to provide customers with a variety of services such software development platforms, servers, storage, and software is a relatively new phenomenon known as cloud computing [6]. In addition, businesses and individuals alike have access to a wealth of tools made possible by cloud computing that allow them to make better use of cloud services without breaking the bank. A company may deploy to the public, private, or hybrid cloud depending on its requirements and

[1]*Associate Professor, Department of CSE, Shri Sant Gajanan Maharaj College of Engineering, Shegaon*
jaimpatil1011@gmail.com
[2]*Assistant Professor, St. Vincent Pallotti College of Engineering and Technology, Nagpur*
schaware@stvincentngp.edu.in
[3]*Assistant Professor,ECE Department Shri Ramdeobaba College of Engineering and Management Nagpur*
tikesh.h@gmail.com
[4]*Assistant Professor, Dept of CSE, SSPACE, Ramnagar, Wardha*
devendra19dandekar@gmail.com
[5]*Dean, Yeshwantrao Chavan College of Engineering Nagpur 440022*
Email- arbhagatpatil@gmail.com
[6]*Associate Professor, Cummins College of Engineering for Women, Nagpur*
amit.thakre@cumminscollege.edu.in

security concerns. The majority of companies are embracing this fast expanding paradigm to fulfil their computing needs and enhance their operations. Consumers and businesses alike may take use of the resources made available by cloud computing, which include storage, network capacity, and server utility for a variety of services and applications. Customers may save money by using cloud platforms, infrastructure, and software as a service instead of buying new gear or software for their businesses [7]. These facilities and cloud-based services are provided by several well-known organizations. The following companies are among the most prominent in this industry:

Search Engine: A plethora of Google services, including Google Docs, email, web analytics, maps, Google Cloud Storage, Google App Engine (for Python, Java, and Go), and many more, are available via Google's private cloud[8].

Microsoft: Users are able to transfer their contents and business intelligence tools to the cloud using Microsoft Office 365 and other online applications, and the company is also making its offline apps accessible in the cloud[9].

Amazon: Amazon Web Services (AWS) is a safe platform for cloud computing that provides features including content delivery, Elastic Cloud Compute (ECC), and Simple Storage Service (SSS) to help companies expand.

Salesforce.com: Users are able to execute apps on the cloud using Salesforce.com. Their product line includes Force.com and vmforce.com, which provide a platform for Java developers to create and launch cloud-based corporate applications.

2. Encryption as a Threat Counter Measure

There were a number of security risks to the Cloud that were highlighted in the preceding section. Here, we take a look at how encryption might help lessen the impact of these dangers.

Cloud Computing Abuse and Malicious Use: The Cloud infrastructure is attractive to attackers because it provides a platform to perform assaults. For the simple reason that it is malleable and can, when needed, access vast amounts of computational power and resources. Certain cryptographic processes may be useful for managing the usage of resources in the cloud and preventing unauthorized access[10]. An example of this would be the use of a customer-generated digital signature to authenticate them on the Cloud without disclosing the secret key. This service provider has no trouble spotting bad actors. The issue persists despite the deployment of encryption, which is ineffective against the Cloud architecture and applies just to data.

Applications and Programming Interfaces That Aren't Secure: The APIs are made available across the network in order to control the Cloud services. These interfaces must be secured to prevent unauthorized users. Cloud communications are protected against eavesdropping by encrypting them[11]. This prevents message counterfeiting and ensures that Cloud management communications remain authentic.

Danger from Inside: Some Cloud providers' staff may have access to stored data in order to govern and manage it. Abuse of such privileges is easy for a malevolent employee to do. Data encryption is one defence against this hazard as it makes the information unintelligible to workers. Afterwards, the data will be protected against insiders who gained unauthorised access. It is important to implement key management procedures with encryption to prevent data decryption in the event that an insider obtains the keys.

Problems with Shared Technology A client might potentially get unauthorized access to the Cloud infrastructure by exploiting a vulnerability in the virtualization hypervisor, since the Cloud is a resource pooling model and the infrastructure is shared among multiple tenants. Cryptographic techniques, such as code signing, may help mitigate this risk by allowing cloud service providers to confirm that apps hosted on their servers are original and unaltered creations from a trusted source[12]. The primary concern here is not data secrecy; hence data encryption won't do much good against this kind of attack.

Data Erosion or Disclosure Encryption is a great tool for keeping data secure in the cloud and preventing unauthorized access, alteration, or erasure. But other dangers will still be unprotected.

The use of authentication technologies and access control measures is crucial in the cloud to prevent account or service hijacking. Because an attacker may get access to client data and use it to launch other assaults if he could modify these techniques. Digital signatures are able to authenticate identification and circumvent attackers' attempts to change access control information. Encryption, however, is ineffective in these cases [13].

Profile of Unknown Risks: In most cases, the Cloud provider does not divulge details on their threat assessment and management processes to the client. Additionally, the provider's security procedures should be considered. Thus, it is incumbent upon the consumer to do their part in bolstering the provider's security measures [14]. Much better than relying on the provider's standards without question for data security management. It is highly recommended that customers encrypt their data before transmitting it to their supplier.

3. Cloud Encryption

After a consumer uploads data to the cloud, he gives up control of the data and gives it to the cloud provider. It follows that encryption is crucial for keeping information private. Depending on the models used by cloud service providers, there are a variety of approaches to the complex process of cloud encryption.

While infrastructure as a service (IaaS) puts the client in charge of security measures and gives them greater control over the infrastructure, software as a service (SaaS) puts them in the least amount of danger. We go over the various Cloud service models and how encryption fits into them here.

Security for software as service platforms Although customers may sometimes take precautions before sending data to the cloud, SaaS providers typically handles all security implementations directly. Encryption in SaaS may be approached from three primary angles.

After data is sent, the cloud provider encrypts it. Once the consumer sends data to the cloud provider, the data is encrypted. The provider may retransmit or keep the encrypted data without worrying about any potential risks to its secrecy. Data transmission between the consumer and the provider is carried out using secure SSL/TLS channels. Data is encrypted before transmission by the customer. After encryption, data is sent to the provider and decrypted when the client gets it. In this scenario, the client has full command over the encryption method and keys[15]. The SaaS programme can only do restricted actions on the encrypted data, including searching, since the provider does not have the decryption key. There may be instances when the encrypted data cannot be read or identified by the SaaS application [16]. An example of this would be an email that is encrypted by the sender before it reaches the email provider (SaaS provider). In this case, the recipients will not get the message.

Between the service provider and the consumer, an encryption system that operates via a network may automatically encrypt the data. It is possible for the third-party proxy to encrypt data sent from the client to the cloud service provider and decrypt data received from the provider[17]. As a result, the provider's encryption storage services are launched independently, relieving the client of the burden of encryption and key management. Trusting the third-party proxy is essential, of course.

4. Objective

Many people who use the cloud are worried that their sensitive information is being sent to a remote location for processing and storage. To allay cloud users' fears, a novel approach to data protection has been given the go light. Therefore, we need a model that addresses almost all of the key issues with data integrity and security, while simultaneously giving the customer more control over their data and offering additional advantages like a low-cost, high-speed cloud environment. In light of the above, our objectives are as follows:

The goal of this research is to better understand how cloud computing handles authentication, data recovery, privacy preservation, and classical cryptography.In order to research and assess the current approaches' computational complexity and security concerns. Its goal is to provide a framework that, in addition to selecting an efficient server for data storage, provides data trustworthiness and a security mechanism.

With the goal of implementing a framework that fixes all those security issues while reducing computation overheads. System dependability and secrecy are greatly impacted by a number of authentication-oriented difficulties that users are compelled to face throughout data transfer, storage, and access. In light of these challenges, it is necessary to provide a new safe approach for efficient data storage and access in the cloud. The primary objective is to study data security concerns and provide a framework to aid with data security. The system can confirm the validity, privacy, and trustworthiness of data, and the suggested work may improve cloud-based client-side data security.

5. Double Authentication Based Cloud Data Security

Parallel computing, distributed computing, grid computing, virtualization, utility computing, software as a service, infrastructure as a service, and platform as a service are all components of cloud computing. Cloud computing is a concept that provides a range of services in the same way as the essential utility services like gas, telephone, water and electricity[18]. Without disclosing details like the delivery method, this strategy allows users to get services according to their needs.The scalability, on-demand nature, and ease of use of cloud computing have contributed to its meteoric rise in popularity in recent years.

Data, operating systems, apps, storage, and processing power are all available on the web as a service in what is referred to as the "cloud." This metaphor describes the web as a place where computing is preinstalled. A Pay-as-You-Go model, cloud computing allows customers to easily access pooled IT resources over the Internet[19]. When it comes to information technology resources like networks, servers, storage, applications, and services, they may be installed with little administration and contacts with service providers. It's also considerably quicker and easier. When compared to conventional methods of computing, cloud computing has several benefits, one of

which is the increased availability of IT resources. By using the IT infrastructure in a Pay-per-Use-On-Demand fashion, users may reap the benefits while avoiding the expense of purchasing unused physical resources. Many individuals now save their data on the cloud. Since the server offers the storage function for the cloud user, a cloud is essentially a collection of several servers that are located remotely and shared by many users. Therefore, in this setting, it is essential to carefully choose a secure server for data storage.

The two main concerns here are ensuring the security of data stored in the cloud and avoiding unauthorised access to that data. The first concern is selecting the most suitable server for storing data in the cloud. The best possible solution can be generated by maximum algorithms, but they are time-consuming. Meta-heuristic approaches such as League Championship Algorithm (LCA), Genetic Algorithm (GA), Ant Colony Algorithm (ACA), BAT algorithm, Cuckoo Search Algorithm (CSA), and Particle Swarm Algorithm (PSA) take a reasonable amount of time. Users are provided with storage services over the internet using cloud computing, allowing them to remotely store their data on the cloud. Both the user and the CSP face a number of security concerns and problems while using remote computing. The CSP provides its services online and uses a variety of network technologies, which might pose security risks. Shared technology vulnerabilities, data breaches, account hijacking, service hijacking, Denial of Service (DoS), and malevolent insiders are among the security concerns that cloud computing encounters.

Cloud computing has brought a new era to computational services by creating an environment that can guarantee, personalise, and provide a reliable service to its customers. Various applications and databases are housed in centralised data centres in this case. Secure data storage and other cloud security characteristics are met by this study, which primarily focuses on compute on the server side and data security. As shown in Figure 1, the double authentication technique provides a visual representation of the security mechanism. An authentication and encryption security system is put in place to ensure that any user data that is received at the server is secure. Every time a user successfully accesses the cloud system, a dynamic server requirement is imposed. Using the Wake Sleep Algorithm in conjunction with the cuckoo search algorithm yields an optimized outcome when selecting servers. One effective way to fit high-dimensional data to a multilayer stochastic generative model is the wake-sleep algorithm. The generative model employs both top-down and bottom-up connections. The former utilise a simple delta rule to train, while the latter use the data to approximate the probability distribution across the hidden units. During the wake-sleep algorithm, the system strives to enhance the congruence between its visual inputs and its internal representations, which are based on its greater understanding of the world. The input image material that the system attempts to recreate during the waking phase is supplied from an external source, such as photographs of handwritten numbers. The deepest memories, on the other hand, use their most stable representation of a concept during sleep as input that they would like the system to regenerate. This framework allows the system to store and access user data from a more internal perspective, depending on the criteria used to select the efficient server. The user may control the different security levels by selecting a security method based on data categorization. Protected data is subject to single-factor authentication, whereas sensitive data is subject to multi-factor authentication. To ensure privacy and security, the owner and user each use their own ECDSA. Using client-side encryption and decryption eliminates the need for a cloud provider to guarantee privacy.

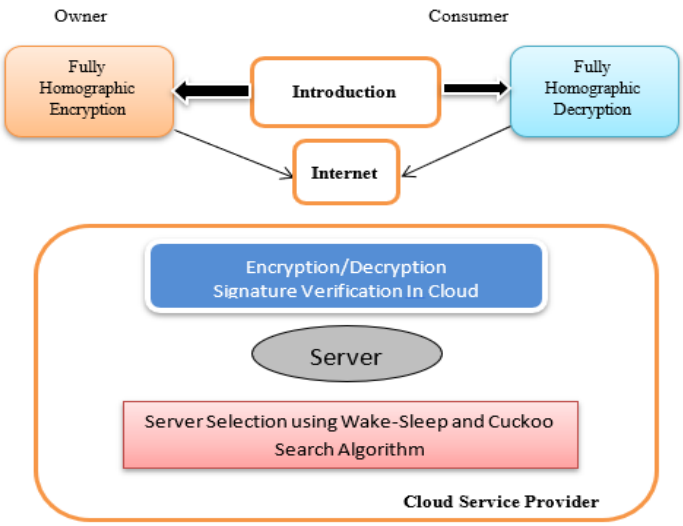

Fig 1 Architecture of double authentication based cloud data security

6. Server Selection Utilizing Wake-Sleep and Cuckoo Search Algorithms

The development of learning algorithms using machine learning and deep learning that can rapidly grasp a concept from a small number of examples while yet effectively generalising to new instances of that concept is a significant problem in the quest to design better secure data security in cloud computing. Our goal here is to find a middle ground between the two extremes: using a big unlabeled server, we will Meta-learn generative parameters and an inductive bias while learning ideas explicitly expressed as stochastic programmers. Our new Wake-Sleep (WS) learning technique is a straightforward combination of cuckoo search and optimum server selection.

By inverting the typical flow of information from the bottom (input) to the top (most abstract layer), our proposed server selection wake sleep method aids in completely homomorphic encryption for safe data. If you want to learn the sleep mode by heart, this is a good step to do.Like a person visualizing a picture or piece of text, the data at the bottom of this inverted network now serves as an abstract representation of the input at the top, which serves as the initial input for the data that flows back down the network, much like an imagined data flow. In order to train its recognition "memory," it incrementally adjusts the network's memories to get a closer approximation to the conceptual representation it meant. Since there is no actual visual input when in sleep mode, it is the same as if it were dreaming or closed its eyes. In this mode, the input is truly located deep into the network. Clearly, the model's picture production outcomes are dictated by external input, and the eye is open, as it was in the initial generating setup. The computational expense of running and cooling the infrastructure inside these datacenters has risen sharply, and in some instances even surpasses the cost of purchasing software or hardware. The global computational cost of datacenters is around $20 billion, according to recent estimates. Clients and suppliers of cloud services alike benefit financially from efforts to reduce the energy consumption of datacenters like these. Reducing computing cost has a substantial impact on datacenter availability, productivity, and reliability; this is in addition to the fact that heat dissipation raises failure rates and huge calculation time. This problem can be solved by combining the wake-sleep algorithm with cuckoo search, which can improve the placement of both outgoing and incoming server requests. In the event that virtual machines are dynamically placed, the wake-sleep-server function will use the CSO algorithm. With the help of the CSO algorithm, the wake-sleep system can better allocate resources in response to server requests sent by cloud providers.

7. Quantum Key Distribution

Cryptographers now have a new tool at their disposal: QKD. This allows for safe key agreement, which is impossible with conventional cryptography, by making the output key completely independent of the input value. It is still required to use other cryptographic primitives, such as authentication, but QKD enables the building of systems with new security characteristics. The two players in QKD, Alice and Bob, acquire and measure a variety of quantum states. In order to determine which measurements may potentially provide secret key bits, they converse with one another (from now on, all communication is classical). Some measurements are eliminated during the filtering process due to incompatibilities between the measurement parameters. Following the correction of mistakes, they make an educated guess as to a security parameter that would describe the level of information that an eavesdropper may possess about their vital data. Since they can't guarantee any degree of anonymity, they won't go forward if the amount exceeds a certain threshold. In the event that it falls below the threshold, they may use privacy amplification to find a shared secret key by eliminating any residual information that the eavesdropper might possess. Part of this time-honored dialogue needs verification to prevent man-in-the-middle attacks. Some portions of the procedure have a very low failure probability. A flow diagram depicting the procedures for the distribution of quantum keys may be seen in Figure 2. After being produced with QKD, a secret key might have several uses. In a one-time pad, it is used as the secret key to provide unconditionally secure encryption. In subsequent rounds of QKD, the key may also be used for classical authentication. Quantum key distribution (QKD) systems are expected to become more dependable, easier to set up, cheaper, and eventually smaller as the field of QKD continues to expand. Eventually, these systems might be miniaturized to the point where they fit on a single circuit board.

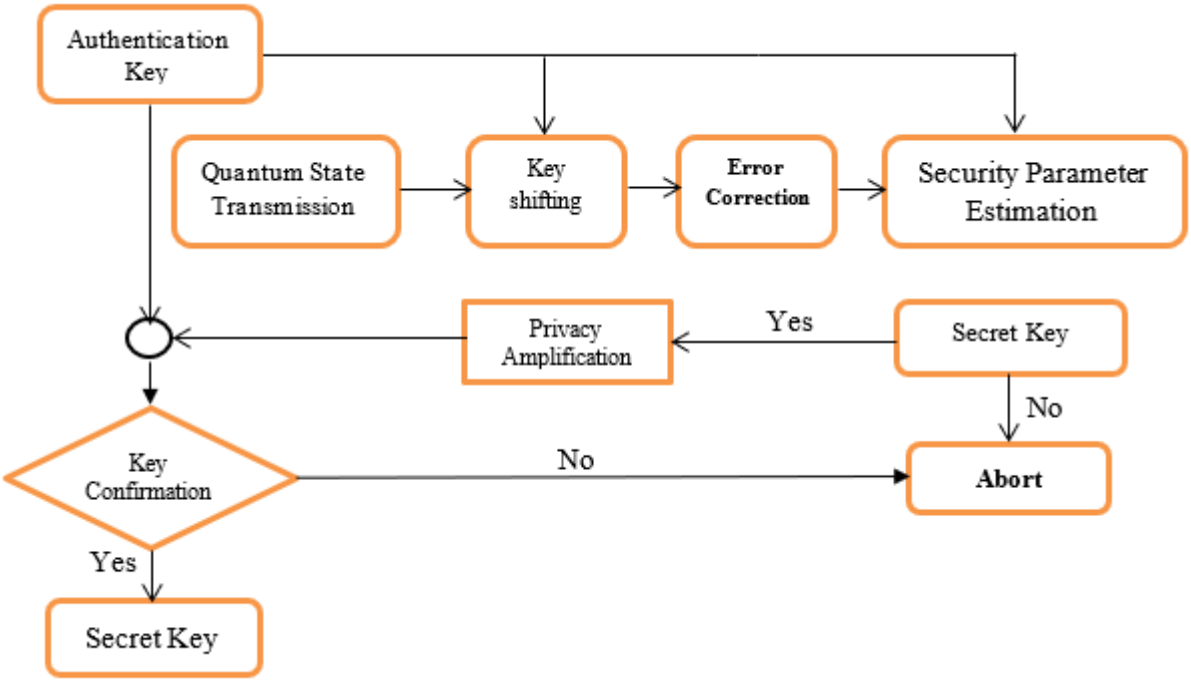

Fig 2. Generalized Stages of quantum key distribution

When a user requests access to encrypted data stored by the owner in the cloud, the owner grants the request. In accordance with the access control policy, the data owner will provide the user with a digital certificate and the decryption key. Most current studies still rely on old cryptography to authorise access to the cloud, but users may have their data secured simply by showing the certificate. The current common encryption techniques may be easily cracked once a large-scale quantum computer is constructed. Cryptography that relies on the assumed difficulty of calculating v functions is facing serious problems as a result of IT advancements. Due to the fact that quantum cryptography, which differs from classical cryptography and is grounded in quantum physics, offers a novel approach to guaranteeing the security of communications, an increasing number of academics are devoting their efforts to studying quantum communication. Some examples of quantum communication include QKD, QSDC, and QSS, as well as secure direct communication. There are two protocols that have found practical use: one, QKD, which uses the Heisenberg uncertainty principle and the quantum non-cloning theorem to generate an unconditional security key; the other, QSDC, which is designed for providing directional information communication only via quantum channel, allows two distant authorised parties to share a secret key through quantum channel and transmit information through classical channel.

8. Conclusion

With the advent of cloud computing, the majority of user data is now kept on remote servers accessible over the Internet. For example, there could be instances when servers are temporarily unavailable, where unauthorized individuals get access to or modify data, and so on. Here, we reviewed the experimental findings and suggested completely homomorphic ECDSA, an efficient framework for server selection that uses a double encryption technique. Furthermore, the Quantum Key Distribution Relying Non-Commutative Encryption Framework (QKDRNCE) was put into place, which combines a secure communication framework with a data repair service and fast secret key generation.

References

[1] Mittal and F. Sidney, "Privacy Preserving based Personal Health Records Sharing Using Rail Fence Data Encryption (RFDE) for Secure Cloud Environment," *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India, 2023, pp. 1-5, doi: 10.1109/ICICACS57338.2023.10099585

[2] S. Mishra and S. Lahoti, "An Efficient User Protected Encryption Storage Algorithm Used in Encrypted Cloud Data," *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India, 2023, pp. 1-5, doi: 10.1109/ICICACS57338.2023.10099610

[3] M. Ramprasath, A. V. Kalpana, T. N. Ravishankar, M. Anand and J. Shobana, "Protected Data Sharing using Attribute Based Encryption for Remote Data Checking in Cloud Environment," *2023 12th International Conference on Advanced Computing (ICoAC)*, Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICoAC59537.2023.10249642.

[4] L. M. Leo, S. Yogalakshmi, A. Veeramuthu, V. Kalist and A. A. Frank Joe, "Experimental Analysis of Data Storage and Integrity Management over Cloud Environment using Integrated Data Security Strategy," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 952-957, doi: 10.1109/ICEARS53579.2022.9751841.

[5] R. K. C and A. Canessane R, "Securing Data storage in Cloud after Migration using Immutable Data Dispersion," *2023 4th International Conference for Emerging Technology (INCET)*, Belgaum, India, 2023, pp. 1-5, doi: 10.1109/INCET57972.2023.10170274.

[6] X. Wang, J. Zhang, Z. Meng, B. Yi, A. Hu and M. Gu, "Research on symmetric encryption and decryption of multi-user shared data for cloud storage environment," *2023 IEEE 6th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, Dalian, China, 2023, pp. 297-301, doi: 10.1109/ICISCAE59047.2023.10393315.

[7] M. M. R and A. T.P, "Novel Weight-Improved Particle Swarm Optimization to Enhance Data Security in Cloud," *2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Kirtipur, Nepal, 2023, pp. 195-200, doi: 10.1109/I-SMAC58438.2023.10290704.

[8] G. Ha, C. Jia, Y. Chen, H. Chen and M. Li, "A Secure Client-Side Deduplication Scheme Based on Updatable Server-Aided Encryption," in *IEEE Transactions on Cloud Computing*, vol. 11, no. 4, pp. 3672-3684, Oct.-Dec. 2023, doi: 10.1109/TCC.2023.3311760.

[9] J. Ning, X. Huang, W. Susilo, K. Liang, X. Liu and Y. Zhang, "Dual Access Control for Cloud-Based Data Storage and Sharing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1036-1048, 1 March-April 2022, doi: 10.1109/TDSC.2020.3011525

[10] J. B K and T. J, "Data Storage Security and Privacy in Cloud Computing," *2022 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE)*, Bangalore, India, 2022, pp. 1-10, doi: 10.1109/ICWITE57052.2022.10176237

[11] B. Rachana, T. Priyanka, K. N. Sahana, T. R. Supritha, B. D. Parameshachari and R. Sunitha, "Detection of polycystic ovarian syndrome using follicle recognition technique", Global Transitions Proceedings, vol. 2, no. 2, pp. 304-308, 2021.

[12] Zhiting Zhang and Peng Zeng, "Large-Universe Attribute-Based Encryption with Public Traceability for Cloud Storage", IEEE Internet of Things Journal (Early Access), 2020.

[13] Gongcheng Hu and Leyou Zhang, "An Expressive "Test-Decrypt-Verify" Attribute-Based Encryption Scheme With Hidden Policy for Smart Medical Cloud", IEEE Systems Journal (Early Access), 2020.

[14] Mitsuhiro Okada and Takayuki Suzuki, "FPGA-accelerated Searchable Encrypted Database Management Systems for Cloud Services", IEEE Transactions on Cloud Computing (Early Access), 2020.

[15] Yinbin Miao and Qiuyun Tong, "Verifiable Searchable Encryption Framework against Insider Keyword-Guessing Attack in Cloud Storage", IEEE Transactions on Cloud Computing (Early Access), 2020

[16] Sheng Cao and Xiaosong Zhang, "Toward Secure Storage in Cloud-based eHealth Systems: A Blockchain-Assisted Approach", IEEE Network, vol. 34, no. 2, March/April 2020.

[17] Ye Tao and Peng Xu, "Secure Data Sharing and Search for Cloud-Edge- Collaborative Storage", IEEE Access, 2019.

[18] G. Hemanth Kumar and G. P. Ramesh, "Reducing power feasting and extend network life time of Io T devices through localization", Int. J. Adv. Sci. Technol, vol. 28, no. 12, pp. 297-305, 2019.

[19] Binanda Sengupta and Sushmita Ruj, "Efficient Proofs of Retrievability with Public Verifiability for Dynamic Cloud Storage", IEEE Transactions on Cloud Computing, 2017.