

Secure and efficient storage approach for cloud environment using hybrid machine learning techniques

Kanav Sadawarti *

Department of Computer Science & Engineering

Mandi Gobindgarh

Punjab 147301

India

Satish Saini [†]

Department of Electronics Communication & Engineering

Mandi Gobindgarh

Punjab 147301

India

Rachit Garg

School of Computer Science and Engineering

Lovely Professional University

Phagwara

Punjab

India

Abstract

Cloud computing is a new way to organize things. Cloud users can store their files that are far away and linked to the web. As a result, personal and critical data are stored in an easily accessible and transferable manner. Hence, its demand is expanding daily. Due to the fact that the user accesses data over the internet, issues about the secrecy and confidentiality have arisen. To address this issue, hybridization employs an encryption technology known as the RSA with 3- DES approach. This article primarily addressed two aspects: data security and storage. The encryption strategy is used to secure cloud data, while the MBFD with WOA & ANN approach is used to store it. Also the utilization of neural network along with the whale optimization model ensures the controlled storage of cloud has been done. The

* E-mail: kanavsadawarti@gmail.com (Corresponding Author)

[†] E-mail: satishsainiece@gmail.com

experiment demonstrates that the suggested cloud system outperforms the present one in terms of energy usage, latency, and SLA breach.

Subject Classification: 68.

Keywords: Service level agreement, Artificial neural network, Data encryption standard, Machine learning, Optimization.

1. Introduction

Cloud computing (CC) is perhaps the most sought full framework. It's made up of a lot of modern tech apps that make it easy for people to store, retrieve, and keep their personal information safe. Cloud services and apps may be accessed through cellular devices such as laptops and smart phones. CC might be regarded the most trustworthy and safe platform in respect of document security. Alternative storage devices, including such cell phones and computers, will be unable to deliver this level of data security owing to the absence of storage capacity and performance [1-3]. Cloud services are used to store and back up any kind of data in an economical, easy-to-use, and quick way [1]. In addition, they can exchange data and keep devices in sync.

There isn't a single set of data storage design qualities that everyone agrees on, and there are different ways to design cloud storage for different cloud infrastructures. On the other hand, cloud storage is made up of many storage devices that are linked together through a file system, network connections, and many other related instruments. This allows customers to use cloud storage. A cloud storage solution is made up of a storage pool, service interfaces, and Service Level Agreement (SLA) [4]. The cloud stores data in an ad hoc manner. As the quantity of data rises, the user's search becomes more complex. On the other hand, if data is organized, the user may readily get the necessary information. As a result, a model must be developed that enables data to be conveniently saved in a cloud-organized format.

Users who purchase applications from suppliers have the opportunity to pick the infrastructure that is best suited to their activities. The cloud provides just a subset of these components, and users have no authority to maintain or control them. For security reasons, the majority of businesses do not disclose any private information. Users who access apps do not have the ability to modify these infrastructure characteristics. Each performance model is predicated on infrastructure choices and control. When a customer requests computing resources from a cloud provider, the

cloud provider provides only basic Virtual Machines (VMs). These virtual computers are dynamically constructed when computing power and network bandwidth are scarce. Almost every cloud provider is developing strategies for effectively managing cloud resources and reducing cloud data centre power usage by powering down unneeded host computers.

CC's main security threats are threats to the integrity, accessibility, and privacy of the service. Cloud services range from data storage to application service planning, and all of them need to be available almost all the time. CC is usually built to be a hard-to-get-into environment that can provide structure, services, process technology, and power when needed [5]. They want to solve problems with security and organize data more effectively with the help of ML algorithms. ML is the use of artificial intelligence to frameworks so that they can learn and grow naturally without having to be explicitly changed [7]. ML is concerned with the advancements in computer initiatives that can learn at their own pace [8].

To ensure the security of stored cloud data, Rivest–Shamir–Adleman (RSA) encryption methods in conjunction with the 3- DES methodology is utilized. The data is saved in the database, then afterwards it is allotted to the user based on MBFD level of severity. Finally, for improvising the security of the suggested cloud model, cross-validation is done utilizing the Whale Optimization Technique (WOA) in conjunction including an Artificial Neural Network (ANN) classification method.

The main outcomes of this paper are:

1. It provides the extensive review of the work that has been done in context of secure cloud storage using ML approaches.
2. It highlights the modified algorithms that are proposed (MBFD with WOA & ANN) under the cloud computing constraints.
3. It executes the analysis of the proposed combination approaches under the factors like SLA, energy and delay with existing model.

The paper is divided in to the sections as per their relevance. The work already done in the context secure cloud storage with ML has been elaborated in 2nd Section. The proposed techniques are defined in Section 3rd. Results and the inference drawn has been defined in Section 4th. Conclusion is highlighted in Section 5th.

2. Related Work

This section summarizes current studies on cloud security offered by many scholars. We focused on three areas in this research: cloud computing security concerns, ML applications in cloud security, and the primary active techniques utilized for cloud services.

2.1 *Cryptographic Approaches Related Work*

The authors of [9] established Heroku as a virtualized environment and then added AES security to Heroku's data. The Advanced Encryption Standard (AES) has traditionally been considered the most effective symmetric approach. The authors used AES-128 bit encryption for data encryption. While doing research and attempting to access data contained in Heroku's database, authentication using a login and a distinct password is necessary. The authors of [10] proposed a security paradigm for restricting access to cloud data by integrating methods, specifically steganography and cryptography. The suggested framework for preserving privacy consists of three stages: hashing data that use the Secure Hash Algorithm (SHA), (ii) encrypting using the AES along with hash code acquired using public-key cryptography, and (iii) combines all data after encryption using Least Significant Bit (LSB) steganography.

Later, researchers developed a unique security technique to increase cloud data security by integrating Blowfish and RSA algorithms, and also introducing a digital signature even during data communication phase [11]. The primary objective of this suggested strategy is to ensure the safe transfer of private data. The combination of symmetric and asymmetric algorithms improves efficiency, while the SHA-2 method increases security when transferring data online. Similarly, the authors of [12] suggested an improved RSA (ERSA) method by augmenting the regular RSA algorithm with two additional prime integers. The suggested technique accelerates encryption and decryption by using prime numbers rather than random numbers. ERSA maintains this performance by partitioning the file into many chunks. Apart from this, implementing the ERSA method simplifies computing and increases security.

The authors of [13] reported a solution derived from a combination of three algorithms: RSA, the Vigenere encryption, and Message Digest (MD)-5. To determine the algorithm's trustworthiness, it is subjected to a variety of assaults, including Gaussian filters. According to the attacking results, the smallest alterations happened in the blurring attack, which has an excellent peak. In [14] proposes a mixed cryptographic solution that

incorporates the advantage of both symmetric and asymmetric to provide a safe environment. This study stress on developing a secure cloud environment that makes use of a multifactor authentication approach that encrypts and hashes data at many levels. The submitted work is simulated using the CloudSim simulator, coupled with the comparing technique.

In [15], a novel paradigm called CryptoGA is offered to address data integrity and privacy concerns. It is built on a Genetic Algorithm (GA). GA is being utilized to produce cryptographic keys that are then utilized in conjunction with a technique to secure the confidentiality and protection of data stored on cloud. For assessment and comparison, well-known and common metrics like execution duration, bandwidth, key length, and avalanche impact are used. Experiments demonstrate that the suggested paradigm protects the confidentiality and authenticity of user data from unauthorized people. As mentioned by the authors [16], it is necessary to understand the algorithms' vulnerabilities, performance, and benefits in order to choose appropriate cryptographic techniques for an application. Their research compares the effectiveness of AES, 3-DES, and RSA encryption algorithms in terms of picture data performance and security in a cloud context. Wide range of analytical ways like cryptanalysis, statistics, and performance monitoring has been used to determine each algorithm's security and reliability efficiency.

Cryptography is widely used, from local institutions and universities to the social media platforms which are normally used. The AES and DES encryption algorithm are the primary focus of the authors' work in [17]. Additionally, they determine which method is best one in terms of time complexity and analyze the disparities between the two methods. The authors of [18] described unique, highly successful, and lightweight homomorphic cryptographic techniques with two levels of encryption. The first layer employs a novel, efficient, and lightweight cryptographic method, while the second layer employs multiplicative homomorphic algorithms to improve data security in CC. The suggested technique is assessed in terms of memory use, computing time, and entropy shift assessment.

Similar kind of research work has been done by the researchers pertaining to the security aspects in the cloud environment [19-23].

2.2 ML Based Secure Cloud Related Work

In this section, we have talked about the work that looked at how ML algorithms could be used to protect the cloud.

In [24], the authors proposed a approach for resolving security vulnerabilities for enhancing the cloud system's performance. The lack of interest in information persists as a result of the information's volatility due to the outsider who collects, controls, and creates it. The authors applied ANNs to the distorted data. The authors of [25] examined the use of ML methods to enhance data security. The topic of distributed computing is highlighted since it is gaining significant momentum, and virtualized servers are gaining recognition as a feasible foundation and solution for massive corporate applications.

The authors of [26] examined the CC threat categorization model's viability for detecting and resolving security concerns using ML methods. Additionally, they presented a strategy for categorizing CC risks based on the capability of using ML techniques to differentiate them. In CC, security concerns and vulnerabilities are addressed using ML algorithms and defensive strategies [27–28].

In [29] authors analyzed ML methods utilize to address security risks pertaining to malwares and CC security. The researchers showed off a blocking model that integrates three ML algorithms that have been chosen because they are good at detecting viruses, like the one shown in this text. The authors of [30] did a thorough review of interruption detection systems which use a supercomputing intuitive method in a mobile cloud environment. The authors of [31] used ANN techniques to forecast fundamental distributed computing security vulnerabilities. A neural network algorithm is utilized to identify security vulnerabilities in a financial institution. ANNs have been utilized to enhance the operation and learning abilities of neural networks.

Similarly, [32] authors highlighted digital attacks in cloud environments which considered as critical for safeguarding cloud arrangement from cyber security threats. A viable solution for identifying digital attacks in cloud infrastructures and distant processing devices is provided. The recommended technique included the use of an ANN. The authors of [33] examined resource management in Mobile Edge Computing (MEC) and how ML may be used to resolve the problem and increase performance. They have used cutting-edge artificial intelligence to accelerate resource advancements in portable edge processing. The authors then suggested a data categorization strategy based on data secrecy in [34]. The authors discussed a method for grouping information that is related to information protection and security.

Similar kind of research work has been done by the researchers pertaining to the security aspects in the cloud environment [35–38]. Also

some prominent work in the direction of secure cloud storage has been done by the researchers [39-45] which is quite useful one.

3. Proposed Methodology

This section describes the suggested security paradigm for cloud data storage. The study is divided into two phases: (1) data storage via an encryption technique and (2) data security with a WOA and an ANN method. The proposed idea has been presented in Figure 1 in the form of architecture.

The data is first gathered from a variety of individuals and then analyzed using the stop word reduction technique. It is a dictionary-based strategy that is used to exclude widely used meaningless terms from user-accepted data, like have, has, is, and am. The functional flowchart for removing stop words is shown in Figure 2.

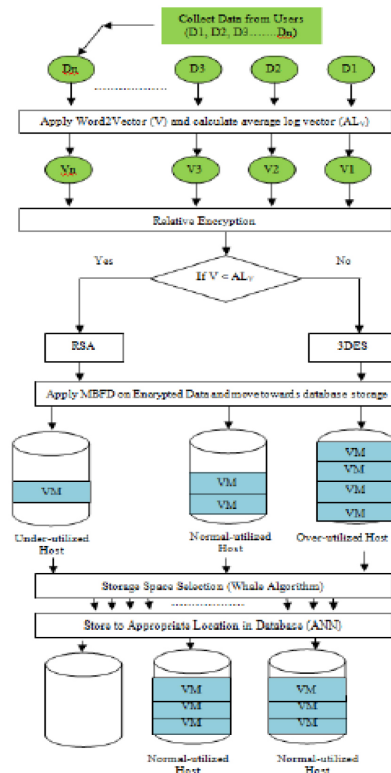


Figure 1
Proposed model architecture

After data preprocessing, it is transferred to the word-to-vector technique. The written material is transformed to a numerical format using this method. Later it is accomplished by determining the ASCII value each text word. Then average value is calculated by calculating the logarithmic value of the each ASCII character. It is considered that if the calculated average value is lesser than the threshold level, the RSA algorithm is used; otherwise, the 3-DES encryption algorithm is used.

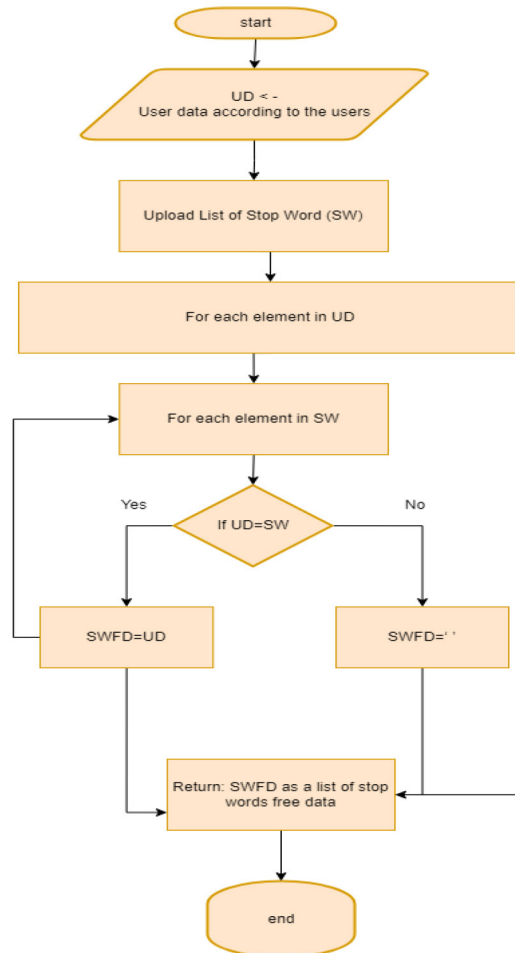


Figure 2
Working flowchart for the stop word removal

After that, the data which is encrypted is used as input for the Modified Best Fit Decreasing (MBFD) technique. Here, this technique prioritized activities based on their energy use. The method for MBFD is shown in Figure 3. We employed whale as an optimization strategy to control data storage. Only those VMs that are required by the user are transferred using the optimization technique.

Following that, the optimization strategy is implemented using WOA and ANN. The Whale is one of the most recent optimization algorithms, having been created in 2016. The method is based on the humpback whale's technique of reproduction. Initially, the whales locate their prey and then surround that place. As the database location is unknown before to the search, the whale algorithm believed the position of the prey has been the most ideal answer.

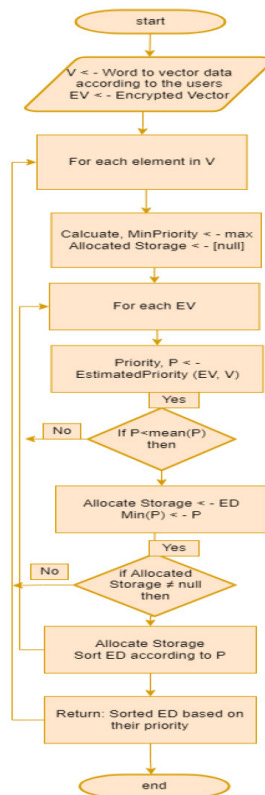


Figure 3

Working flowchart for the modified MBFD approach

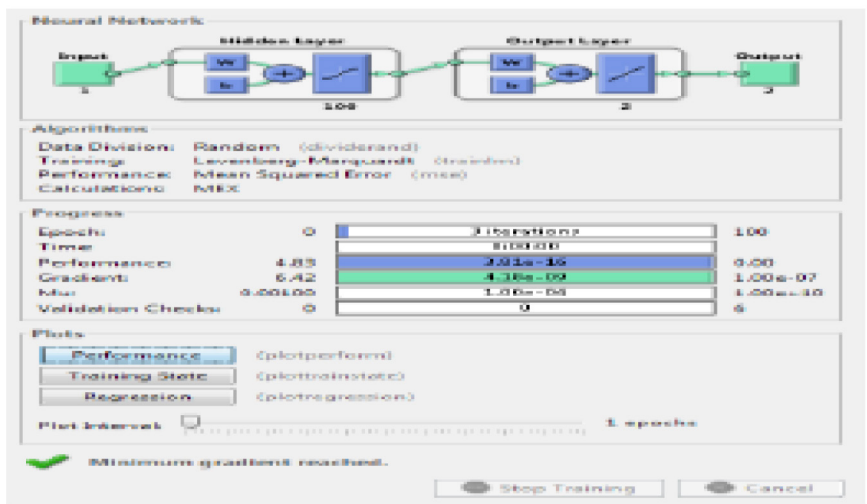


Figure 4
Training process representation

WOA aides in the selection of a suitable database region depends on the fitness value. The improved data of the user is then sent into the ANN, which then trained the system to determine whether database space is being over or underused. Figure 4 illustrates the trained structure of an ANN. The training of the ANN is being done using the hidden and the output layers. To analyze the performance of the model mean square error is being analyzed.

4. Results and Analysis

In order to evaluate the efficiency of the developed security cloud model, MBFD, WOA, and ANN approaches have been used to analyze latency, energy usage, and SLA violation metrics. The calculated results for the fluctuation of user request count in comparison to energy consumption for the proposed MBFD and other suggested techniques combining WOA and ANN are presented in Figure 5.

In a datacenter, servers use energy in two ways: static power and dynamic. Static power is often considered to be constant while the system is switched on. Recent study indicates that the quantity of energy used by a server is linked to the quantity of CPU time available.

The most critical characteristic in the cloud infrastructure is energy consumption, which must be reduced in order to conserve energy. The

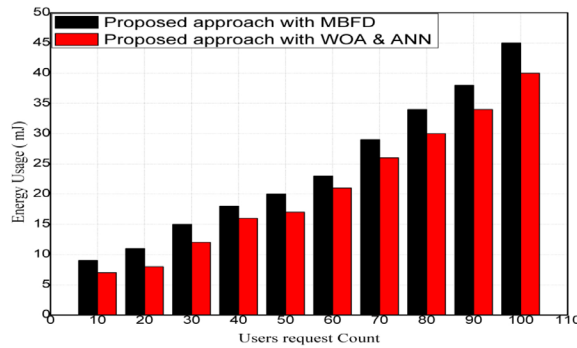


Figure 5

Variation of energy usage with request count

parameter is analyzed in this case in relation to the count of user requests. Because the volume of traffic from users varies between 10 and 100, the database evaluates how much power each operation consumes in order to position them correctly. When seen in Figure 5, as user demands grow, energy usage increases proportionately. The value of average energy spent by the MBFD strategy is 24.2 mJ, whereas the WOA & ANN approach consumes 21.1 mJ. Thus, when WOA is combined with the ANN technique, energy usage is reduced by 3.1 percent. This is due to the optimization method utilized in the latter, which results in a more efficient use of energy.

To determine whether or whether the data transferred to the cloud is safe and to assign enough storage space, the latency parameter is analyzed. In practice, it is observed that data traffic in a cloud environment

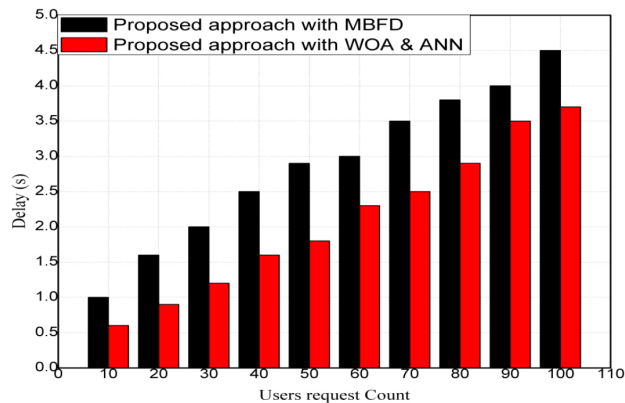


Figure 6

Variation of delay with request count

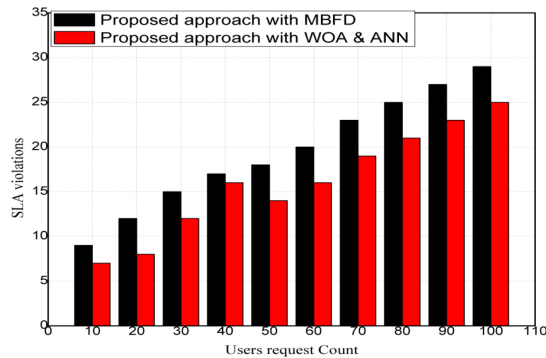


Figure 7

Variation of SLA violation with request count

is rising daily and will eventually reach a critical level, affecting the cloud system's performance. The latency in cloud computing is caused by a many variables, comprising the amount of user requests, the quantity of uploaded data, and the channel's speed, all of which contribute to latency or bottleneck. The latency has been reduced in this case by combining WOA and ANN as a ML strategy, as seen in Figure 6. The average delay measured while utilizing basic MBFD and when employing WOA & ANN approaches is 2.88 s and 2.1 s, respectively. It has been deduced that when WOA is combined with the ANN technique, the velocity of accurately recording of data on the database is boosted by.78 percent.

The average power usage of each allocation is used to determine SLA breaches. If any allocation's power usage exceeds this overall average, the SLA is breached. SLAs are critical for ensuring that the Cloud Service Provider's (CSP) services meet the client's requirements. If the CSP violates the services, the providers will be required to compensate its subscribers. This study employs an ANN technique to analyze and decrease SLA breaches. As seen in Figure 7, the suggested technique delivers superior offerings to its consumers. The value of average SLA violation recorded while using MBFD and WOA & ANN is 19.5 and 16.1, respectively. Again it is inferred that the WOA & ANN technique resulted in a 3.4 percent decrease in SLA violation when compared to the basic MBFD algorithm.

5. Conclusion

We provide unique security approach with controlled storage space for a CC environment in this article. The security structure is implemented

utilizing RSA and a 3-DES technique. The data which is encrypted is then categorized according to its energy usage order using the MBFD algorithm. The WOA technique was used to tackle the storage space selection issue. An ANN-based categorization method has been used to find the right area in a database, which is the area that isn't being used. Thus, a cloud storage paradigm that is both safe and efficient has been devised. Energy usage, latency, and SLA violation have been used to determine performance. It has been deduced that using WOA with the ANN technique results in a 3.1 percent decrease in energy usage when compared to the MBFD strategy. Similarly, when WOA is combined with the ANN technique, the speed of accurately putting data into the database is boosted by 78 percent. Additionally, 3.4 percent reductions in SLA violation are investigated using the WOA and ANN approaches versus the standard MBFD method. The suggested cloud model outperforms a basic or typical cloud computing system in terms of performance. In the future, deep neural networks will be used to identify malicious URLs and registry keys that have been legitimately prepared. Although the study of ML using crowd sourcing has made tremendous progress in recent years, there will still be certain fundamental difficulties that need to be addressed in the future.

References

- [1] Sun, X., Wang, Z., Wu, Y., Che, H., & Jiang, H. A price-aware congestion control protocol for cloud services. *Journal of Cloud Computing*, 10(1), 1-15 (2021).
- [2] Al-Said Ahmad, A., & Andras, P. Scalability resilience framework using application-level fault injection for cloud-based software services. *Journal of Cloud Computing*, 11(1), 1-13 (2022).
- [3] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. A review of machine learning algorithms for cloud computing security. *Electronics*, 9(9), 1379 (2020).
- [4] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. A review of machine learning algorithms for cloud computing security. *Electronics*, 9(9), 1379 (2020).
- [5] Duc, T. L., Leiva, R. G., Casari, P., & Östberg, P. O. Machine learning methods for reliable resource provisioning in edge-cloud computing: A survey. *ACM Computing Surveys (CSUR)*, 52(5), 1-39 (2019).

- [6] Li, K., Gibson, C., Ho, D., Zhou, Q., Kim, J., Buhisi, O., ... & Gerber, M. Assessment of machine learning algorithms in cloud computing frameworks. In *2013 IEEE Systems and Information Engineering Design Symposium*, pp. 98-103. IEEE (2013, April).
- [7] Callara, M., & Wira, P. User behavior analysis with machine learning techniques in cloud computing architectures. In *2018 International Conference on Applied Smart Systems (ICASS)*, pp. 1-6. IEEE (2018, November).
- [8] Oh, M., Park, S., Kim, S., & Chae, H. Machine learning-based analysis of multi-omics data on the cloud for investigating gene regulations. *Briefings in bioinformatics*, 22(1), 66-76 (2021).
- [9] Lee, B. H., Dewi, E. K., & Wajdi, M. F. Data security in cloud computing using AES under HEROKU cloud. In *2018 27th wireless and optical communication conference (WOCC)*, pp. 1-5. IEEE (2018, April).
- [10] Ebrahim, M. A., El-Maddah, I. A., & Mohamed, H. K. Hybrid model for cloud data security using steganography. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, pp. 135-140. IEEE (2017, December).
- [11] Timothy, D. P., & Santra, A. K. A hybrid cryptography algorithm for cloud computing security. In *2017 International conference on microelectronic devices, circuits and systems (ICMDCS)*, pp. 1-5. IEEE (2017, August).
- [12] Amalarethinam, I. G., & Leena, H. M. Enhanced RSA algorithm with varying key sizes for data security in cloud. In *2017 World Congress on Computing and Communication Technologies (WCCCT)*, pp. 172-175. IEEE (2017, February).
- [13] Ardy, R. D., Indriani, O. R., Sari, C. A., & Rachmawanto, E. H., Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). In *2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS)*, pp. 87-92. IEEE (2017, November).
- [14] Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. Cloud security ecosystem for data security and privacy. In *2017 7th International conference on cloud computing, data science & engineering-confluence*, pp. 288-292. IEEE (2017, January).
- [15] Tahir, M., Sardaraz, M., Mehmood, Z., & Muhammad, S. CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. *Cluster Computing*, 24(2), 739-752 (2021).

- [16] Rahul, B., & Kuppusamy, K. Efficiency Analysis of Cryptographic Algorithms for Image Data Security at Cloud Environment. *IETE Journal of Research*, 1-12 (2021).
- [17] Reshma, R. S., Anjusha, P. P., & Anisha, G. S. Implementing the Comparative Analysis of AES and DES Crypt Algorithm in Cloud Computing. In *Computer Networks and Inventive Communication Technologies*, pp. 325-332. Springer, Singapore (2022).
- [18] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks* (2022).
- [19] Ajmal, A., Ibrar, S., & Amin, R. Cloud computing platform: Performance analysis of prominent cryptographic algorithms. *Concurrency and Computation: Practice and Experience*, e6938.
- [20] Murad, S. H., & Rahouma, K. H. Hybrid Cryptography for Cloud Security: Methodologies and Designs. In *Digital Transformation Technology*, pp. 129-140. Springer, Singapore (2022).
- [21] Sohal, M., & Sharma, S. BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. *Journal of King Saud University-Computer and Information Sciences*, 34(1), 1417-1425 (2022).
- [22] Bakro, M., Bisoy, S. K., Patel, A. K., & Naal, M. A. Hybrid Blockchain-Enabled Security in Cloud Storage Infrastructure Using ECC and AES Algorithms. In *Blockchain based Internet of Things*, pp. 139-170. Springer, Singapore (2022).
- [23] Devmane, V., Lande, B. K., Joglekar, J., & Hiran, D. Preserving Data Security in Cloud Environment Using an Adaptive Homomorphic Blockchain Technique. *Arabian Journal for Science and Engineering*, 1-14 (2022).
- [24] Khan, A. N., Fan, M. Y., Malik, A., & Memon, R. A. Learning from privacy preserved encrypted data on cloud through supervised and unsupervised machine learning. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1-5. IEEE (2019, January).
- [25] Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. Feasibility of supervised machine learning for cloud security. In *2016 International Conference on Information Science and Security (ICISS)*, pp. 1-5. IEEE (2016, December).

- [26] Liu, Y., Sun, Y. L., Ryoo, J., Rizvi, S., & Vasilakos, A. V. A survey of security and privacy challenges in cloud computing: solutions and future directions. *Journal of Computing Science and Engineering*, 9(3), 119-133 (2015).
- [27] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, 63(2), 561-592 (2013).
- [28] Behl, A., & Behl, K. An analysis of cloud computing security issues. In 2012 world congress on information and communication technologies, pp. 109-114. IEEE (2012, October).
- [29] Selamat, N., & Ali, F. Comparison of malware detection techniques using machine learning algorithm. *Indones. J. Electr. Eng. Comput. Sci*, 16, 435 (2019).
- [30] Shamshirband, S., Fathi, M., Chronopoulos, A. T., Montieri, A., Palumbo, F., & Pescapè, A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications*, 55, 102582 (2020).
- [31] Elzamly, A., & Hussin, B. Classification of critical cloud computing security issues for banking organizations: A cloud Delphi study. *International Journal of Grid and Distributed Computing*, 9(8), 137-158 (2016).
- [32] Guha, S., Yau, S. S., & Buduru, A. B. Attack detection in cloud infrastructures using artificial neural network with genetic feature selection. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 414-419. IEEE (2016, August).
- [33] Zamzam, M., Elshabrawy, T., & Ashour, M., Resource management using machine learning in mobile edge computing: a survey. In 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), pp. 112-117. IEEE (2019, December).
- [34] Zardari, M. A., Jung, L. T., & Zakaria, N. K-NN classifier for data confidentiality in cloud computing. In 2014 International Conference on Computer and Information Sciences (ICCOINS), pp. 1-6. IEEE (2014, June).
- [35] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. Deep Learning Based Homomorphic Secure

- Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. *Sensors*, 22(2), 528 (2022).
- [36] Sajid, F., Hassan, M. A., Khan, A. A., Rizwan, M., Kryvinska, N., Vincent, K., & Khan, I. U. Secure and Efficient Data Storage Operations by Using Intelligent Classification Technique and RSA Algorithm in IoT-Based Cloud Computing. *Scientific Programming*, (2022).
- [37] Anees, A., Hussain, I., Khokhar, U. M., Ahmed, F., & Shaukat, S. Machine Learning and Applied Cryptography. *Security and Communication Networks*, (2022).
- [38] Oke, A., Kushwaha, A., Agrawal, M., Sahai, U., & Raman, R. A Novel Approach to Encrypt Data Using Deep Neural Networks. In *Advances in Distributed Computing and Machine Learning*, pp. 467-475. Springer, Singapore (2022).
- [39] Hossain, M. J., Xu, C., Zhang, Y., Zhang, X., & Li, W. LAMA: A secure lattice-based authentication scheme for cloud storage against misbehaved private key generator. *Journal of Ambient Intelligence and Humanized Computing*, 1-17 (2022).
- [40] Sharma, P., Jindal, R., & Borah, M. D. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. *The Journal of Supercomputing*, 1-29 (2022).
- [41] Suresh, S. A., & Priyadarsini, R. J. Design of Maintaining Data Security on IoT Data Transferred Through IoT Gateway System to Cloud Storage. *International Journal of Computer Networks and Applications*, 9(1), 135-149 (2022).
- [42] Tian, J., & Zhang, T. Secure and effective assured deletion scheme with orderly overwriting for cloud data. *The Journal of Supercomputing*, 1-29 (2022).
- [43] Neela, K. L., & Kavitha, V. An Improved RSA Technique with Efficient Data Integrity Verification for Outsourcing Database in Cloud. *Wireless Personal Communications*, 1-18 (2022).
- [44] Li, S., Xu, C., Zhang, Y., Du, Y., & Chen, K. Blockchain-Based Transparent Integrity Auditing and Encrypted Deduplication for Cloud Storage. *IEEE Transactions on Services Computing* (2022).
- [45] Fu, Z., Wang, Y., Sun, X., & Zhang, X. Semantic and secure search over encrypted outsourcing cloud based on BERT. *Frontiers of Computer Science*, 16(2), 1-8 (2022).