International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

*Volume **14** Issue **1s** Year **2022** Page **136:152***

A Framework for Uncertain Cloud Data Security and Recovery Based on Hybrid Multi-User Medical Decision Learning Patterns

V. Devi Satya Sri[1*], Srikanth Vemuru[2]

[1]Research Scholar, [2]Professor

[1,2]Department CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India-522502

vdevisatyasri@gmail.com, vsrikanth@kluniversity.in

Article History

Received: 13 July 2022
Revised: 20 September 2022
Accepted: 30 October 2022

Abstract

Machine learning has been supporting real-time cloud based medical computing systems. However, most of the computing servers are independent of data security and recovery scheme in multiple virtual machines due to high computing cost and time. Also, this cloud based medical applications require static security parameters for cloud data security. Cloud based medical applications require multiple servers to store medical records or machine learning patterns for decision making. Due to high Uncertain computational memory and time, these cloud systems require an efficient data security framework to provide strong data access control among the multiple users. In this work, a hybrid cloud data security framework is developed to improve the data security on the large machine learning patterns in real-time cloud computing environment. This work is implemented in two phases' i.e. data replication phase and multi-user data access security phase. Initially, machine decision patterns are replicated among the multiple servers for Uncertain data recovering phase. In the multi-access cloud data security framework, a hybrid multi-access key based data encryption and decryption model is implemented on the large machine learning medical patterns for data recovery and security process. Experimental results proved that the present two-phase data recovering, and security framework has better computational efficiency than the conventional approaches on large medical decision patterns.

Keywords: Cloud Computing, Cloud Uncertain Data Security, Data Partitioning, Medical Patterns, Multi-User Data Access.

1. Introduction

CLOUD computing can give patients, physicians, healthcare workers, and administrators with quick access to a variety of healthcare materials, apps, and solutions. Cloud computing may assist hospitals and emergency medical providers overcome financial hurdles to universal adoption of EHR and offer the infrastructure required to ensure the supply of patient information by lowering the initial investment and reducing the expenses of data centres, equipment, and IT. A variety of different parties are wary of

entrusting their own sensitive data to the cloud due to security concerns. Certain resource-constrained entities rely on the cloud to complete a difficult calculation operation. An efficient and effective way to safeguarding privacy is required. Protecting this sensitive data on the cloud is critical. To safeguard this sensitive data in the cloud, many encryption techniques are used. Encryption is a time-consuming and difficult operation. The encryption process oversees restricting access to cypher messages that have been processed. The goal of holomorphic encryption is to aid the whole computing process [1]. It is also responsible for enforcing data integrity and confidentiality restrictions. The single user-based system is a key flaw in the holomorphic encryption technique. Multiple users are never supported by traditional holomorphic encryption techniques. The amount of procedures that may be performed on cypher messages is restricted. To accommodate alternative cypher text calculations, a fully holomorphic encryption technique is devised. On the other hand, it significantly increases the total calculation overhead. As a result, in real-world situations, this approach cannot be used. Customers may store their information on cloud servers from anywhere, and these cloud servers are responsible for providing services as needed. The two primary cloud computing organisations are cloud service providers and cloud customers, both of which originate from different areas. In the period of remote data storage in cloud computing, security and privacy are two important concerns that must be addressed. Users must set up a secure data access control system before uploading sensitive personal data to the cloud. It is critical to have a secure encryption system as well as a fine-grained access control mechanism for corporate data sharing across cloud servers. As a result, a new method known as the Attribute-based encryption system is produced by combining both of the preceding systems [2]. The following are the key objectives of the suggested models: Cloud data security for large amounts of data: Costly bilinear pairing and slower processing speed of resource restricted devices are issues in the encryption process. [3] The cost issue can be resolved by decomposition of encryption phase into two parts such as offline phase and online phase. In case user wants to share the data stored in cloud through the network, these sensitive confidential data become more vulnerable to be exposed. Attribute based encryption is introduced as an advanced method for enhancing the data security and privacy of cloud data significantly. It permits every individual user to specify access policies for the encryption process. The access policies are responsible for managing and controlling the access rights of each user to access cloud data. If the attributes of user's private key are checked with access policy successfully, then that user is allowed to access a file stored in cloud storage. These access policies include some user's characteristics like date of birth, gender, or domain/application specific attributes. There are some special types of files which can be decrypted at only particular time. The geographical location of cloud user's also varies very frequently from time to time. It is now possible for customers to store their data in a third-party data centre using cloud computing. Cloud computing depends on pooled energy assets to ensure consistency and efficiency. Since it minimises the amount of information while boosting its efficacy and reducing costs, it represents an important turning point in software research. The security of user data, for example, was jeopardised as a result. Algorithms were developed to provide the highest level of security. Only if the information is comprehensive, private, and accessible can the information be accessed. [4]

A customer's comfort and satisfaction in storing third-party information about an information centre is the most significant need. Many cryptographic methods are invented to obtain this level of security. Since then, other variants of hashing have emerged. A hash function is a common way to encrypt data when it is intercepted by a hacking system. The MD5 hacking algorithm was created in 1991 by MIT Professor Ronald Rivest. Utilizing a 128-bit hash function, this approach is vulnerable to a brute-force attack using two different combinations of a current Intel 2.6 GHz Pentium 4 CPU. Even this hash value may be corrupted in seconds by colliding attacks. Digital signatures, digital time stamping, digital authenticity, digital steganography, pseudo-numbering, and other safety-related operations rely on cryptographic hash functions, which are the primary cryptographic tools. The block cypher and the flow cypher are greatly outclassed by the hash features used in a wide variety of data processing programmes. Hash functions may be found in all security software and are quite helpful. Using a hash function, numerical data may be compressed into a smaller size. With a self-assured hash task contribution and a consistently re-adjustable output, the digest and hash value are other names for the hash character properties. For cloud data security, attribute-based encryption is one of the most scalable approaches. ABE is the name given to this approach.

In this technique, each client is assigned a unique set of allowed attribute sets, rules, and a privacy key to keep their information private. [5] It's been argued multiple times in the previous several centuries that attribute-based encryption would be useful. The data size of the space attribute is quadratically limited to security measures since the key space and attribute set are established in the setup phase. When performing an ABE operation, the access tree buildings decrypt the secret key, the private key, and any cypher text that may be present. It's possible to decode encrypted text if certain criteria are met, but only then. CP-notion ABE's is essentially the opposite of KP-method. ABE's CP-ABE serves as a foundational component in several other systems due to its adaptability. Since KP-ABE has no control over decryption freedoms, it has no disadvantages. This previous strategy's issue has been addressed here. In addition, real-world scenarios are included. This approach, however, has a serious flaw: It cannot be applied in a business environment. As a result of inflexibility and poor efficiency, this defect is present. A single set of characteristics is required for the whole decryption procedure. Because of this, users have the option of selecting one or more characteristics from a predetermined selection. The ABE paradigm was used to construct a hierarchical attribute-based encryption scheme. Hierarchical structure served as a metaphor for the whole method. The root master oversees key creation, and he works with numerous other domain masters to accomplish this. Every domain manager must deal with many corporate customers. In the cloud enterprise and proxy re-encryption domains, this method might be used. Asymmetric cryptography may be performed using public-key cryptography. Anyone may use the public key to encrypt messages, which can only be decoded by someone with the corresponding private key. Attribute-based encryption is a sort of public-key cryptography that allows anyone to decode emails if their decryption key is compatible with the ciphertext access policy. Internet verifiers aren't necessary to protect data from unauthorised access when it's encrypted. It was found that the typical hashing method has several limitations, such as the need for a large quantity of resources. As a workaround, they combined Tandem-DM with the Discrete Chaotic Map Network (DCMN). Instead of employing floating points, their algorithm relies on integer fields. Simulating their hypothesis, they found that it was more efficient and less prone to collisions than the standard method they were comparing it with. Parallel Chaotic Neural Networks were used to construct an enhanced version of the chaotic hashing technology. Using simulations, it has been shown that their suggested function is collision-resistant and performs better. Semi-Collision attacks were also described as a new sort of assault. To avoid this, additional investigation is required. [6]

Ellipses and chaotic systems were used in the development of an algorithm for a new digital signature. They used one-way hashing, two-dimensional hyper-chaotic mapping, and a public key method to create their innovative solution. There is no risk of a key duplication attack because of their algorithm's design. It is possible to use the proposed method in real-world situations since it is safe, trustworthy, and easy. Chaotic-based secure hash algorithms have been fully examined in this area. There are advantages and disadvantages to each strategy that we have examined and determined. One-way hashing was also presented as a possible solution to the problem of collisions It is possible in the future to improve various algorithms, such as MD4, MD5, SHA, and whirlpool. When they looked into it, they found a lot of study focused on computer usefulness and innovative applications had already been done in this area. Many preexisting methods for determining cloud storage patterns were examined, which resulted in storage and sharing issues. Data encryption, border management, and data proofing are all made easier as a result of this. To do all of these tasks, the view management system is used. Data availability and secure data exchange are only two of the many benefits of this method. To ensure the privacy of each user, a secure border separates their personal view from the rest of the system. There are two methods to RBAC: DAC and MAC. They are combined to bring together their imperative qualities. Sender's request for public key is what initiates both encryption and decryption in public key-based encryption, according to its core idea (KDC). It is signed and sent to the requester via the Public Key Infrastructure (PKI). If the sender does not have the public key, the encryption procedure will fail. The communication is encrypted and transmitted across an unencrypted cloud channel. To decode the cypher text message sent by the sender, the recipient must have access to the private key. Some drawbacks of this method include: - the sender must connect with PKI before communicating with the recipient. It is a four-step process: - setup, key generation, encryption, and decryption. Information security checks and steps to protect data and facilities may be included in cloud

computing security measures, as well as approaches. Security in the cloud has become a huge issue since it is so vulnerable to attack. As a result, cloud technology has additional safeguards in place. It's time to do rid of the usual safety architecture since customers don't want to deal with it themselves. Weakest organization's safety requirements are met via a cloud-based technology. Typically, users lose physical control of information when they outsource it to an untrusted cloud service provider and hand over complete control of the information to a distant server. Vulnerabilities may be exploited in the cloud, even if the server is powerful and secure. This might put the confidentiality of information, the integrity of data, and the accessibility of information at risk. To protect their reputations, dishonest service providers constantly hide the flaws in their systems. By removing less accessed information, cloud storage room is sometimes improved [7].

2. Relate Works

Xiao, et al., developed a novel method and dubbed it HASE by expanding the KP-ABE scheme. In a cloud environment, it provides data security and user revocation. Users' access rights, the accountability of their secret key, as well as the data overheads were all reduced by combining the Lazy Re-encryption and Proxy Re-encryption principles. To enable fine-grained access control policies, this approach takes a high calculation time as compared to others, which is a drawback that may be improved upon in the future. A dynamic re-encrypted ciphertext policy-attribute-based encryption approach was developed by Quan, J. The primary goal of this method is cloud-based file sharing security. To distribute the burden of data maintenance and control, cloud service providers may re-encrypt shared data and provide it to verified users. The suggested solution is suitable for secure data exchange in a cloud setting if access control and plain text are kept secret. CP-ABE security was not compromised by the new method, and the new method was found to be very efficient. The properties are weighted according to their importance. Because qualities are so important, this strategy is more suited to cloud systems than other methods. This technique is only a little bit more realistic. A threshold access structure is used in this method. It is possible to expand this method by including additional access structures [8]. With the use of holomorphic encryption, Gao created Cipher Text Policy-Attribute Based Encryption. CP-ABE, the Searchable Encryption, was the solution they presented. Users may get the data they need from cloud-stored files without having to download the encryption text thanks to this technology. Security and efficiency were assessed, and the researchers determined that this technique improves security and reduces computing time compared to typical CP-ABE systems. Using ABE on the cloud, Abdoun has come up with a novel file-sharing system The most prevalent services offered by service providers are file-sharing systems. Considering the widespread usage of cloud-based file sharing, a safe and efficient method must be in place [9]. Their cloud file system was integrated into ABE without the need for pairing (CP-ABE-WP). They created a Secure File Sharing System (SSFS) that is both more secure and more efficient using this method. New hashing schemes that permit parallelism were proposed by Taha after analysing the time-consuming nature of single threaded hashing. The suggested method uses multi-core computers, which means it takes less time. They further claimed that their method is more secure, faster, and more efficient than other methods. For the CP-ABE approach, the data owner does not know who has access to the data, which is its only flaw. Access to fine-grained information is therefore reduced. Before exchanging data, the data owner conducts a thorough investigation of all data access regulations, users, and their qualities. The original data of the users may be retrieved using this way. Only if the attribute access is equal to the user access may access be granted to the user [10]. Validation of their hypothesis and evaluation of the suggested work were carried out. That strategy solves the problem of fine-grained access, according to their findings. The results are superior to those achieved by conventional methods. One-to-many communications with multiple privileges may be implemented using this mechanism. They used a quadratic residue strategy based on large data to build a novel approach to ABE. Bilinear pairing, quadratic residue, and lattices are the fundamental principles of the suggested approaches. It is a variation of Identity-Based Encryption that uses traits rather than IDs to protect data. Using a group of users' ciphertext, the authors describe their system as an improved access control mechanism. There is a single access structure for all the users. When it comes to ABE, the bilinear pairing

notion is more often applied. A basic arithmetic theorem may be applied to the whole notion. The main issue with this method is that, in the event of a squared value, it discards unlawful user access.
The RSA-PKE approach was proposed by Fujisakiet.al and referred to as access control reinforcement for searchable encryption schemes. Their main goal was to improve the security of data access. Searchable encryption and access control mechanisms are combined in this system. This technique ensures both cloud and user secrecy. It also prevents unauthorised individuals from accessing data. The hybrid technique is more vulnerable to assaults in terms of ACAS features. The authors addressed this issue by implementing a security filter on the client site. They combined the concepts of the SSE and KP-ABE programmes into one. In addition to multi-user access control and secrecy, this technique also preserves ACAS features. They looked at the results based on their search and indexing strategies. In addition, they asserted that indexation time is directly related to the collection's size. In other words, when indexation time increases, the size of the collection grows as well. The search time is not affected by the amount of results. For the Dynamic Re-encoded Cipher Text Policy-based Encryption Model [11], they created an additional feature. This model's major goal is to guarantee that data may be shared wirelessly. Re-encrypting and forwarding shared information to authorised users allows cellular service providers to share load management and control of information owners. Access control and plain text are kept secret using the suggested technology in a wireless context, making it suitable for secure data transfer. They were able to demonstrate that the new technique did not compromise the security of CP-ABE and that it was very efficient. The qualities are prioritised in accordance with their relative weights. In a wireless context, the importance of qualities makes this technique more practical and acceptable than other alternatives. That method is only a little bit closer to the real-world reality. A threshold access is used in this method. This technique may be further developed to incorporate more structures for gaining access. Using Cipher Text Policy-Attribute Based Encryption [12] and homomorphic encryption. Consumers may receive the information they need from documents stored on the wireless server without downloading the encryption text thanks to their method. File sharing systems are the most frequent services supplied by service providers. Without pairing, they created a wireless file system that was merged with ABE (CP-ABE-WP). A more secure and efficient Secure File Sharing System was created because of this method (SSFS). There is a problem with single-threaded hashing, and they have come up with a novel hashing algorithm that can be used in parallel [13]. With multi-core computers, the Given suggested technique may be implemented in a shorter amount of time. They further claimed that their method is more secure, faster, and more efficient. They found just one flaw in the CP-ABE model: the data owner has no notion who first used the data. As a result, the amount of fine-grained access lowers. To prevent the data owner from exchanging information without first checking all connections between data access policies users and their qualities, this tool was developed. The original data users' information may be retrieved using this way. For a user to have access, they must have access to the same attribute as the user. They carried out experiments to verify their hypothesis and evaluated the ideas put forward. They discovered that the problem of fine-grained access is resolved using the method. The end outcome is better than any other method now in use. One-to-many conversations between several people may be improved by applying this strategy. They used a Big Data-based quadratic residue strategy to build a novel approach to ABE. Bilinear pairing, quadratic residues, and lattices form the basis of the suggested approach. It is a kind of Identity-Based Encryption that considers the identity set of characteristics. Attribute-Based Encryption According to the authors, their technique is an improved access control scheme for calculating cypher text for user groups. The group of users is incorporated in a single access structure. The bilinear pairing notion is employed more often in ABE. The fundamental theorem of arithmetic can be applied to the entire concept. However, when an unauthorised user access is squared away, this model fails miserably [14]. For searchable encryption schemes, the SE-ACAS technique is a means of enhancing access control. To improve data access control, this was the primary goal. Both searchable encryptions and access control techniques are included in this merged mechanism. Confidentiality is ensured from both a wireless and user perspective using this method. It also restricts access to data for unauthorised users. The ACAS properties of the hybrid approach are more vulnerable to attack. To address this issue, the authors implemented a secure filter on the client site. They combined the ideas of SSE-1 and KP-ABE schemes. Multi-user security, confidentiality, and preservation of ACAS

properties are all advantages to this approach.... They evaluated the results based on their search and indexing strategy. In addition, they stated that indexation time is directly related to the size of the collection's database. In other words, as indexation time increases, the collection grows as well. Volume does not affect how long it takes to search. Ring signature schemes based on the ElGamal signature scheme concept were proposed by. The actual user identity in this scheme is not disclosed to the cloud provider. Also, the authors have generated the signature. They proposed the improved RSA version called the dual RSA algorithm. They have generated two different key pairs in this scheme that have the same private and public exponent. In key generation, this dual RSA algorithm insures additional computational complexity. [15] Presented a modified version of AES with dual-core architecture consisting of two distinct cores for the encryption and decryption process. This architecture also includes a key generation unit with a 32-bit data path to generate the round keys for the encryption process which proved that this scheme provides security against attacks of random adaptive message. The limitation of this scheme is the complexity of its design due to its requirement for more hardware resources. H had suggested a proxy re- encryption scheme. [16] And a decentralized erasure code was integrated to formulate a secure distributed storage system. This scheme allows the user to forward data to other servers or users from the cloud storage servers without downloading the data. This technique of proxy re-encryption supports operations of encoding and forwarding over encrypted messages. However, in implementing the encoding and forwarding the operations this method entails additional overhead. Presented a retrievable method of data perturbation to safeguard the privacy of outsourced data outsourcing in cloud computing. This method involves four steps such as the introduction of an upgraded random generator to produce an accurate "noise" the use of an algorithm to disturb the original data by adding noise, the use of an algorithm for information retrieval to generate the original data from the disturbed data and, finally, the combination of the disturbance method with the access control procedure to ensure access. By experiments, the authors have proven that their scheme correctly, efficiently, and securely disrupting static data, but failed to handle dynamic data. A new block cipher, symmetric encryption called the 2-Keys symmetric encryption algorithm, was proposed to address the above problems. This algorithm has proven to be the best one for massive data storage encryption than the existing encryption algorithms. Based on the experimental analysis, this encryption algorithm is shown to incur less overhead computational and communication and consume less time for encryption and decryption compared to existing methods of encryption. Additionally, this encryption algorithm can also be used to encrypt audio and video content and can be applied to dynamically changing data. [14] Proposed a remedy for the integrity check problem. It is stated that instead of calculating the MAC of the entire data, the data user divides the file F into several data blocks {b1, b2, ... bj}, calculates a MAC for each block bj: ÿj = MACsk(j), stores both the original data file F and the MACs{~j} to the remote cloud server, removes the local copy of the file storing only the secret key sk in the local storage. During the verification process, the verifier will retrieve a set of arbitrarily selected data blocks and the respective MACs. The verifier then re-computes the MAC of the retrieved data blocks using the secret key and compares the re-computed MACs with the MAC values which the remote server receives. The problem with this approach is that it is possible to verify the integrity of only the specific data blocks retrieved from the server, and not the integrity of all data. MAC-based approaches to remote integrity verification suffer from high overhead communication [17].

Described a model that overwhelms some of the restrictions of previously discussed PDP schemes: limited number of file verifications, expensive client and server computation, overhead storage of verifiers, lack of block support for less verification and high complexity communication. The DO fragments the file F into blocks within this scheme {b1, b2, BM} and generates metadata (a tag) for each block of data that can be used to verify. The DO stores the original data file in the remote cloud server and maintains only the meta-data in his local storage. Then, the DO may delete the original data file from the local copy. The remote cloud server provides evidence of data accuracy by responding to the challenge messages sent by the verifier. The limitation of the scheme is that only a random subset of stored data blocks can be checked by the verifier, and not all data. HVTs (Homomomorphic Verifiable Tags) or HLAs (Homomorphic Linear Authenticators) are the basic building blocks for the PDP schemes [18] In this work the authors demonstrated the differences in private verifiability between the concepts of public verifiability. In the

former case anyone-who knows the data owner's public key can challenge the remote server. But the latter allows the auditing task only to be carried out by the original DO. A tag of size 1024 bits needs to be generated in this HVT scheme to achieve a security level of 80-bit. In [19] Ateniese et al. Demonstrated that from holomorphic identification protocols the Holomorphic Linear Authenticators can be generated. They provided a transformation technique for generating these HLAs and demonstrated a method for converting the HLA into a PDP scheme. In [18], Pasupuleti et al presented a cooperative PDP protocol that supports multi-cloud batch auditing, and suggested a dynamic auditing technique in. However, supporting the batch auditing process bearing multiple data owners is unbelievable for these schemes. As the parameters used by each owner to generate the data tags are different, it is impossible to combine the data tags from multiple data owners to provide batch auditing. And during batch auditing an additional trusted organizer is also required to generate and transfer the commitment to the data owner. [20] Suggested a demonstrable possession model that replicates data across remote cloud servers to perform cloud dynamic operations. This scheme fulfils the confidentiality, integrity, and availability of the cloud-saved data. [21] Suggested an effective Cloud computing remote data possession scheme. It has some advantages: cost efficient computation and communication, verification without the need for original data to be copied locally, requiring only small challenges and answers. But that the remote possession scheme has the constraint on the number of challenges cloud users are facing. Cloud instances, available resources, storage attributes, and load balancing may be used to create the goal function of the resource allocation issue. It's also important to keep track of the current condition of server resources in real-time scheduling. This resource allocation system relies heavily on monitoring and resource discovery methods. For resource optimization methods, it is essential to know the services, resources, and their condition to pick those that fulfil all cloud specifications [22]

3. Propose Model

Data replication could happen when the same data is saved on several storage devices or replication if the same computer work is carried out repeatedly. It is the process of automatically distributing and maintaining synchronous distribution of copies of data and database objects among multiple cloud instances. A classifier may learn a set of rules, or a criterion for judgement, using machine learning and a collection of labelled data annotated by an expert. When compared to a system that depends only on human input, this method allows for greater scalability and lower expenses. Most of the research in machine learning-based categorization of medical data focused on binary classifiers. In other words, build a classifier from a set of positive and negative examples to then deduce the membership of a medical data in a class. Up to now, the approach in dealing with a corpus that has medical data belonging to multiple classes has been to build a separate binary classifier for each class in the corpus and then to aggregate the results of each binary classification. Classification can take many forms, from fully automated human intervention systems to semi-automatic systems that use a hybrid human machine approach. As one of the most important chronic illnesses, microarray data set takes a long time to evolve from moderate symptoms into severe disease and death. Generally, medical data includes a list of cancer patches and their associated diseases [23]. Detecting those who are at high risk for this illness is quite tough for the doctor to conduct. In addition, patients' prior medical history and understanding of the condition help them to spot it more quickly. The structural modifications of airways may create remodelling of the wall, and this may lead to decrease in luminal diameter. Again, it is also responsible for thickening of the airway wall. Emphysema can be defined as a serious chronic respiratory disease in which the destruction of alveolar walls is caused without any fibrosis. For classifying the KNN and decision tree classification, the first method takes into consideration the equal number of features of each dimensionality reduction method and for each dimension reduction method, the second method consideration is the minimum number of features needed to give maximum accuracy in classification. The concept of set-feature selection is extended. A mapping strategy is developed to fuse the information of each gene by the MF-GE system, which has enhanced sample classification accuracy. An effective gene selections algorithm (NMI), Correlation-based Selection Feature (CFS), and Particle Swarm Optimization (PSO) are proposed to be integrated into a set technique, and SVM with leave-one-out cross

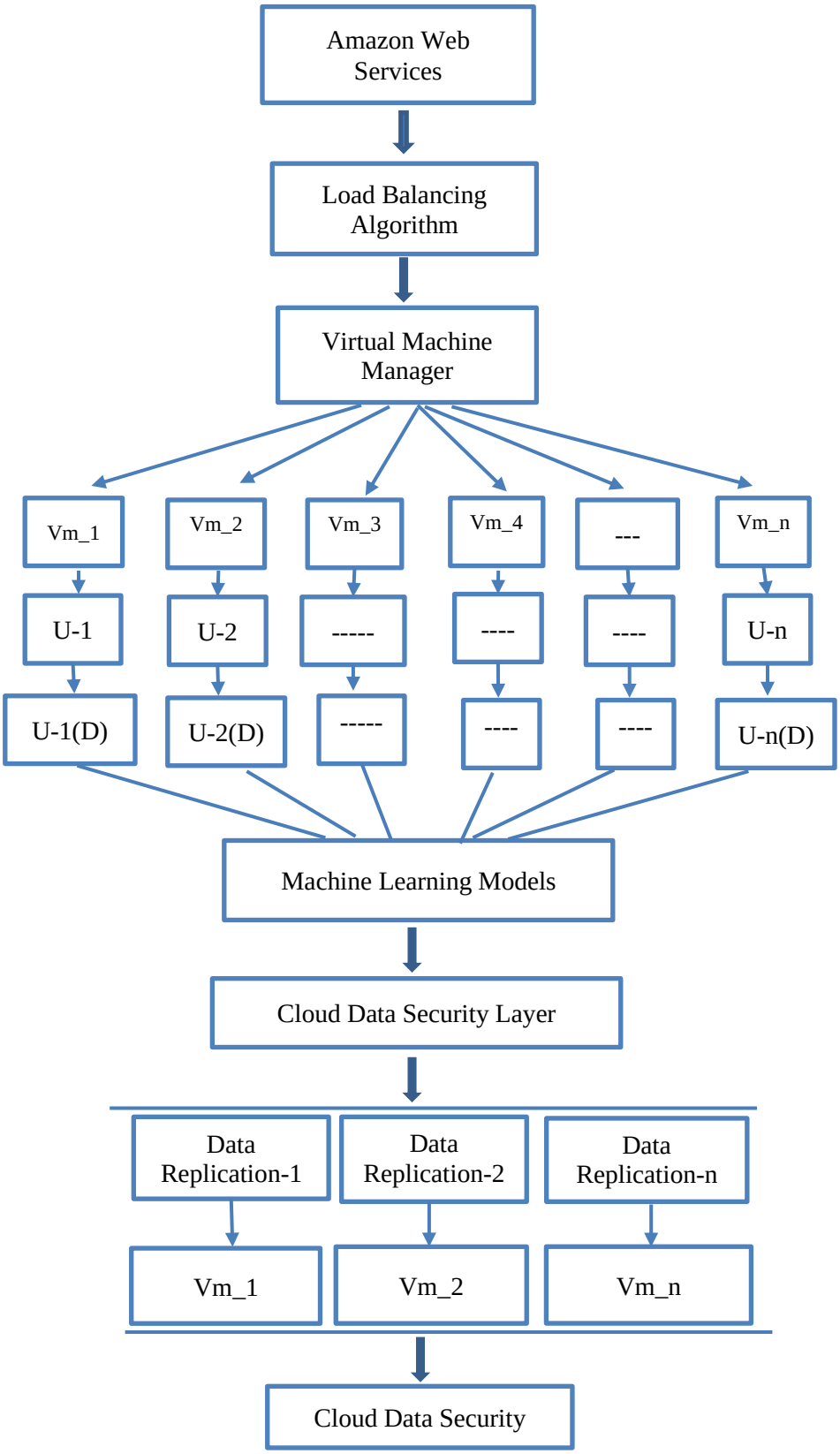

Figure 1. Proposed multiple data partitioning load balancing parameter selection.

validation is used as a classification [24]. Fix and Hodges, which is one of the simplest and most popular classifications, was first introduced to the k-nearest neighbor method (k-NNN). As a learner, the k-NN has a simple strategy. The k-NN classification has two phases, the first phase consists of the determination of the k-neighbors and the second phase of class definition using the neighbors. It maintains all training instances instead of generating an explicit model. This takes a test example feature in a vector form and finds the Euclidean distance from each example to the vector representation. From the figure 1, initially, different virtual machines are taken as input to each user. Since, each user has k number of virtual machines; each user's data is partitioned by using the data partitioning algorithm. Each data part in the data partitioning algorithm is given to integrity model before storing into the VM as shown in Fig 1. In this framework, initially, decision tree patterns are generated using the machine learning approaches. These patterns are replicated using the multiple servers for data recovery process. Finally, these patterns are secured using the integrated and data security algorithm [25]. In this work, a hybrid non-linear kernel based SVM algorithm is implemented on the data for disease prediction. Here, a hybrid kernel function is used to compute the high dimensional disease class prediction on the filtered medical data. Finally, proposed two hybrid classifiers c1 and c2 are used in the boosting approach for better classification. Boosting classifier is used to test the majority voting of each test sample using the hybrid base classifiers c1 andc2.

Algorithm 1: Block wise Uncertain Data Replication

Input: clouded files
Output: data files with user access policies. Procedure:

1. To each file in the cloud user datafiles
2. Partition the data into k blocks
3. To each block B(i) in k block each with 1024 bits
4. Do
5. Let V_ID be the cloud virtual machine ID with available data zones.
6. Compute user's access policy using algorithm 2 as U_P(VM_ID,B(i)).
7. Compute each user's secret nonce by using the cyclic group parameters as

Let Zr, G1, G2 are randomized cyclic group parameters with generator a.

8. Replicate the block to each VM in the VM List
9. Done

Algorithm 2: User access policy generator

1. Initialize secret key K.
2. Partition the input data M into blocks with size 8.
3. Block Processing

Divide the block into 32bit size sub-blocks for n non-line non transformation in the proposed model;
Sp[]=Block Partition[s/32];
Fori=0 to len(SP) Do
While(r<NR) // r current round Do
Perform Sunblock processing (SP[i])
Done
Done

4. Sub block processing
   For each byte in SP [i]
   Do

$$mat\_y = |N|.\frac{e^{-\sum k-\mu/\rho}}{2\rho} \; ; \rho > 0$$

$$\eta = Norm(mat\_y);$$

$$gdf(\eta) = \frac{\lambda^{\alpha}\lambda^{\alpha-t}\log(-\lambda x)}{\exp(\alpha)}, for x > 0$$

$$\mathrm{h1} = \mathrm{sp[i]};$$
$$\mathrm{h2} = \mathrm{f(sp[i])} = \log\left(\frac{\lambda e^{-\lambda(\mathrm{sp[i]}-\mathrm{t})}}{(1+e^{-\lambda(\mathrm{sp[i]}-\mathrm{t})})^2} * \mathrm{position}(\eta).\mathrm{mean}\right)$$
$$\mathrm{h3} = \mathrm{bytes}(mat\_y)$$
$$\mathrm{H[i]} = \mathrm{h1\hat{}h2\hat{}\ h3}$$

Done

In the algorithm 2, each user's access control policy is updated by using the policy generator. In this algorithm, a secret key and input data is partitioned to find the block wise access control as shown in steps 1-3. In the step4, data each block is sub-partitioned to compute the access policy in the step 5. In the step 5, each sub-block partition is used to compute the user's access policy by using the hash value.

3.1 Multi-User CP-ABE Model

In the proposed fast multi-user cipher text attribute-based encryption model, an optimized key generation process and encoding process are included in the conventional CP-ABE model. This model includes four phases i.e integrity based multi-user setup process, integrity-based encryption process, non-linear secret key generation process and multi-user purchase ordering integrity verification and decryption process. According to this approach, multiple parties are responsible for distribution of user attributes [26]. Multi-authority the ABE method relies on a single central authority and many attribute authorities. The value dk is assigned to each attribute. The basic steps in the MA-ABE technique are:

1. Setup: In trusted institutions like key authorities, the setup algorithm is performed. It recognizes the security parameter as input, and together with a few other secret keys it generates a public key. The algorithm also provides a government scheme key and a master secret key for the main agency.
2. Key attribute generation: Usually an attribute agency performs this algorithm. In addition to the user's GID and a variety of characteristics in the authority domain, it contains the secret authority key and authority dk value. For each consumer, this method generates a unique secret code.
3. At the core agency, all the algorithms have been put into place. For each client, a secret key is generated based on the customer's true secret key and their GID.
4. To encrypt the signal, this technique alters the original signal's format. A starting message in plain language, a key to the government's plan, and a number of characteristics for each power are considered inputs. Cryptographic text generated by an algorithm (i.e. the edited format of the initial plain text message).
5. Decryption: This method, like the one used by most consumers, is deterministic. For a collection of Au characteristics, it accepts code text as input and decryption keys. The message results for all k officials with algorithm m.

3.2 Multi-User setup process

In the initialization process, different types of user specific randomized hash keys are generated with variable sizes such as 2048, 4096 etc. These keys are generated dynamically based on the medical data. Here,

G1, G2, Zp represent the cyclic group elements for key Initialization process

LetG1, $G2$, $Zp\ a\ re$ randomized cyclic bilinear pairing numbers

$KS = Ur$ {(2048), (4096)};

3.3 Integrity based Encryption Process

In this phase, a randomized cyclic pairing element, multi- user MEDICAL as attributes, each user integrity value as policies are used to encrypt the medical heterogeneous Uncertain data using the access tree structure. Let P represents list of policies, Pubk represents public key, s=Zr, m and Zn are the cyclic groups. The attribute list, public key and policies are used as input to generate the two-security metrics as the output.

Here α, β are the cyclic group cloud hardware parameters which are relative prime to the multiplicative group. Here C1 and C2 are computed.

$$F\ (m) = \frac{r1}{\pi[(m - r1)^2 + r2^2]}$$

Cipher text CT={ c_1,cs={ g_hat_alpha.(Zn)^s ,m. K }, Atree,c={ Pubk.h.(Zn) }, AccessTree T,c_2, F(ms)}

3.4 Non-linear secret key generation process

In this phase, a set of attributes and integrity values as policies and master_key are used to construct a complex private key for the decryption process

3.5 Multi-User Purchase Ordering Integrity Verification

During the decryption process, cypher text, a secret key, the Access tree, and policies are used to decode the input data provided by the Sample Tonsils Data & Sample Trauma Dataset. These datasets provide comprehensive details on the individual being analyzed. (See table 1 & 2)

Table 1. Sample Tonsils Data

Age	Gender	Throat Pain	Couch	fever	DiS	Swelling	BP	Cold	Out come
55	0	1	0	1	0	1	0	1	No
65	0	1	1	1	0	1	1	1	Yes
43	0	0	0	1	1	0	0	0	No
76	0	1	0	1	0	1	0	1	No
34	1	0	0	1	0	0	1	0	No
74	0	1	0	1	0	0	0	1	No
74	0	0	1	0	1	0	0	1	No
80	0	0	1	1	1	1	0	0	Yes
71	1	1	0	0	1	0	1	0	No
63	0	1	1	0	1	0	1	1	No
51	1	1	0	0	0	1	1	1	No
85	0	0	0	0	1	1	0	0	No
41	1	1	0	1	1	1	0	0	No
77	1	0	1	1	0	0	0	1	No
63	1	0	1	0	1	1	0	1	Yes
46	0	1	1	0	0	0	0	1	No
46	1	1	0	1	0	1	0	1	No
77	0	0	1	0	1	1	1	0	Yes
67	0	1	0	0	1	0	0	1	No
41	0	1	1	1	1	0	1	1	No
44	0	1	1	1	1	0	1	1	No
38	1	1	1	0	0	1	1	1	Yes
82	0	0	0	0	1	1	1	0	No
69	0	0	1	0	1	0	0	0	No

Table 2. Sample Trauma Dataset

ISS	**NISS**	**PS14**	**Age**	**WBC [109/L]_T1**	**NEUT [109/L]_T1**	**LYMPH [109/L]_T1**	**MONO [109/L]_T1**
11	11	97.21493	41	26.16	21.95	1.6	2.58
9	22	99.59795	22	8.28	4.21	3.53	0.33
14	17	99.10462	47	9.24	4.52	3.73	0.45
4	12	99.85114	38	11.54	6.37	4.18	0.65

24	34	87.32603	78	17.43	12.48	3.46	1.1
10	11	98.71743	32	7.74	3.42	3.57	0.53
16	29	93.84556	45	19.75	8	9.96	1.18
9	18	99.76171	19	7.54	4.77	2.15	0.51
20	29	99.09567	27	11.6	4.89	5.75	0.73
16	16	99.58353	26	12.9	8.27	3.83	0.66
29	41	99.14808	24	7.89	4	2.94	0.55
25	34	96.59351	29	15.43	10.16	4.24	0.77
24	34	98.87315	41	15.06	7.37	6.79	0.65
9	27	99.76171	40	5.7	3.17	1.67	0.64
34	34	76.86534	20	20.06	16.6	2.67	0.57
5	9	91.23877	45	0	0	0	0
25	57	98.82117	24	10.28	5.94	3.23	0.91
45	75	50.03899	75	13.81	10.12	2.54	1
50	66	19.20794	64	11.49	4.32	6.54	0.51
45	66	69.21967	19	11.86	4.03	7	0.69
20	29	76.77983	71	9.53	5.24	3.69	0.45
29	75	52.17855	75	8.84	6.15	1.94	0.57
42	66	23.97323	54	10.04	4.57	4.68	0.57
50	66	98.20634	20	13.94	6.77	5.87	1.01
29	57	56.55968	22	13.53	8.34	4.3	0.8
29	41	51.9769	20	20.61	15.06	4.26	1.06
29	41	61.4512	56	14.09	10.2	2.91	0.9
38	75	88.43839	25	12.82	6.46	5.63	0.46
38	43	74.10602	66	11.39	4.55	5.76	0.5
29	57	34.3041	49	4.75	3.14	1.24	0.34
9	22	85.15661	90	10.14	3.02	6.26	0.71

4. Expérimental Résulta

Experimental results are performed on the data cloud computing environment with user's Uncertain datasets. In this study, Amazon AWS cloud server is used to find the block wise replication process in the available cloud virtual machines. In these experimental results, each user's machine learning patterns are used as input data for replication process. These patterns are derived from the medical databases using filtered based classification models. Table1 and Table2 consist of the sample Tonsils and Trauma data sets [27].

Table 3. Comparative analysis of present model to the conventional models on multi-User cloud Trauma Cloud data patterns

Test Patter ns	**SHA512+CP -ABE**	**MD5+KPA B E**	**MD5+CP -ABE**	**Multi Use r-CP-ABE**
TP-1	6503	6569	6256	5302
TP-2	6304	6709	6777	5043
TP-3	6389	6646	6061	5015
TP-4	5912	6498	6077	5330

TP-5	6566	6791	6673	5117
TP-6	6378	6048	6765	5322
TP-7	5991	6612	5834	5294
TP-8	5906	6347	6407	5052
TP-9	5977	6542	6078	5292
TP-10	6316	6732	6743	4788
TP-11	6845	6830	6201	5102
TP-12	6761	6495	6092	5288
TP-13	5929	6058	6151	4831
TP-14	6532	6854	6459	5229
TP-15	6267	6618	6125	5004
TP-16	6697	6245	5866	5026
TP-17	6052	6716	5890	5125
TP-18	6729	6114	5978	4768
TP-19	6775	6632	6453	5148
TP-20	6145	6156	6070	5152

Table 3, (Comparative analysis of present model to the conventional models on multi-User cloud Trauma Cloud data patterns) illustrates the comparative analysis of present model to the conventional model on different cloud tonsils patterns. Here, proposed encryption model has better runtime (ms) than the conventional approaches on the different test medical patterns. In this table, different test patterns are taken into consideration for security in each virtual machine.

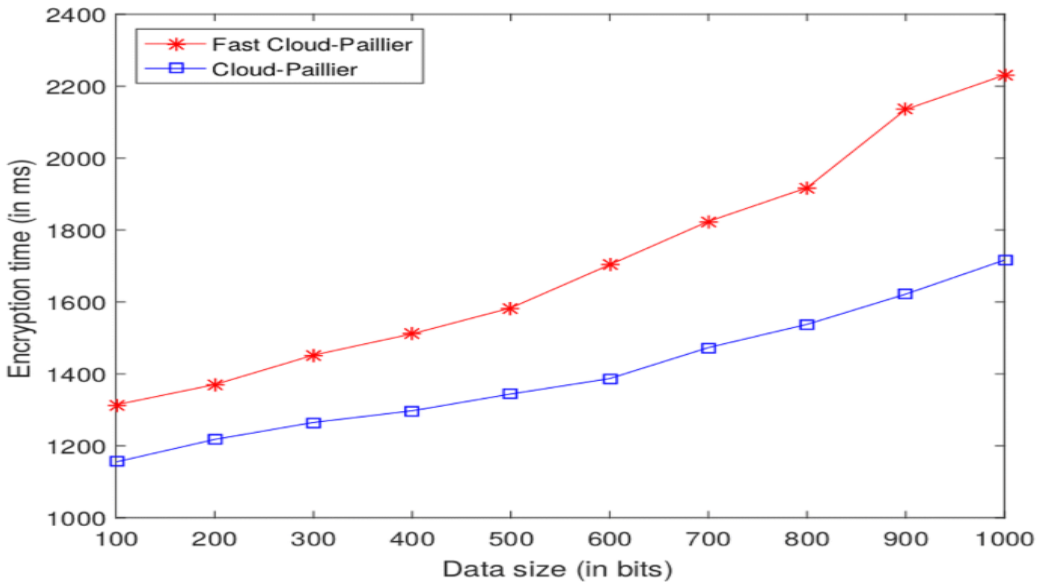

Figure (2). Homomorphic schemes for protecting on multi-user cloud Tonsils Cloud data patterns.

Fig 2 illustrates the homomorphic schemes for protecting on multi-user cloud tonsils cloud data patterns for sensitive data in cloud analytics. Here, proposed encryption model has better runtime (ms) than the

conventional approaches on the different test medical patterns in this figure, different test patterns are taken into consideration for security in each virtual machine.

Table 4. Comparative analysis of present integrity model to the conventional models on multi-user cloud Trauma Cloud data patterns

Test Patterns	SHA512	MD5	Whirlpool	Multi User-Integrity
TP-1	4003	3914	4303	3338
TP-2	4780	4867	4109	3105
TP-3	4851	3855	4775	3045
TP-4	4454	4256	4493	2923
TP-5	4651	4461	4748	3203
TP-6	4608	4089	3953	3145
TP-7	4664	4108	4148	2833
TP-8	4360	4603	4097	2917
TP-9	4093	4624	4382	2996
TP-10	4500	4666	4351	3082
TP-11	4262	4814	3903	2942
TP-12	4847	4378	3893	3069
TP-13	4625	4518	4596	3247
TP-14	4406	4303	3843	3048
TP-15	4284	4458	4779	3245
TP-16	4623	4390	4331	2963
TP-17	4256	4027	4798	3045
TP-18	4845	4864	3849	2791
TP-19	3875	4612	4636	3151
TP-20	4336	4345	4349	3120

Table 4 illustrates the comparative analysis of present integrity model to the conventional model on different cloud tonsils patterns. Here, proposed integrity model has better runtime (ms) than the conventional approaches on the different test medical patterns in this table, different test patterns are taken into consideration for security in each virtual machine.

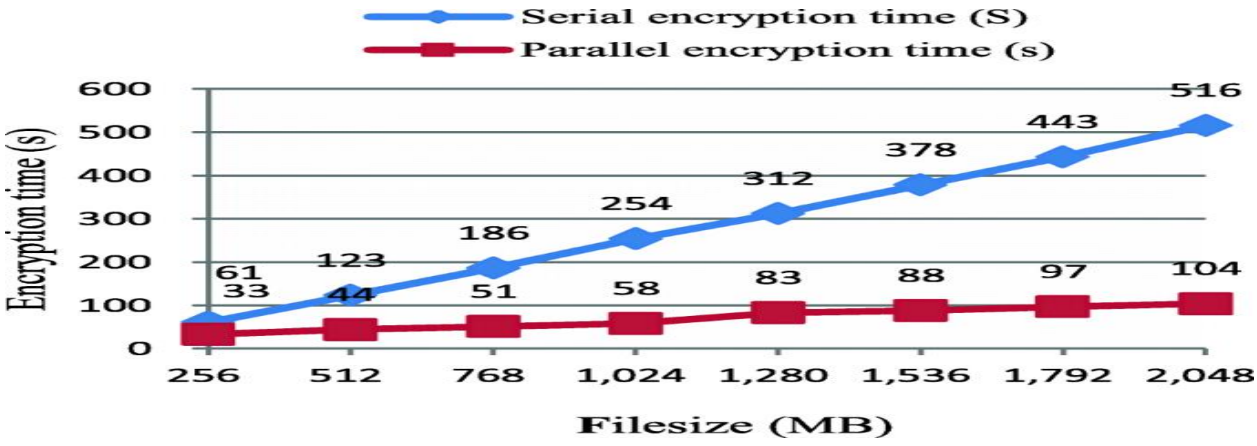

Figure 3. Security preserving encryption scheme for cloud data patterns

Fig 3 illustrates the security preserving encryption scheme for cloud data patterns. Here, proposed integrity model has better runtime (ms) than the conventional approaches on the different test medical patterns in this table; different test patterns are taken into consideration for security in each virtual machine.

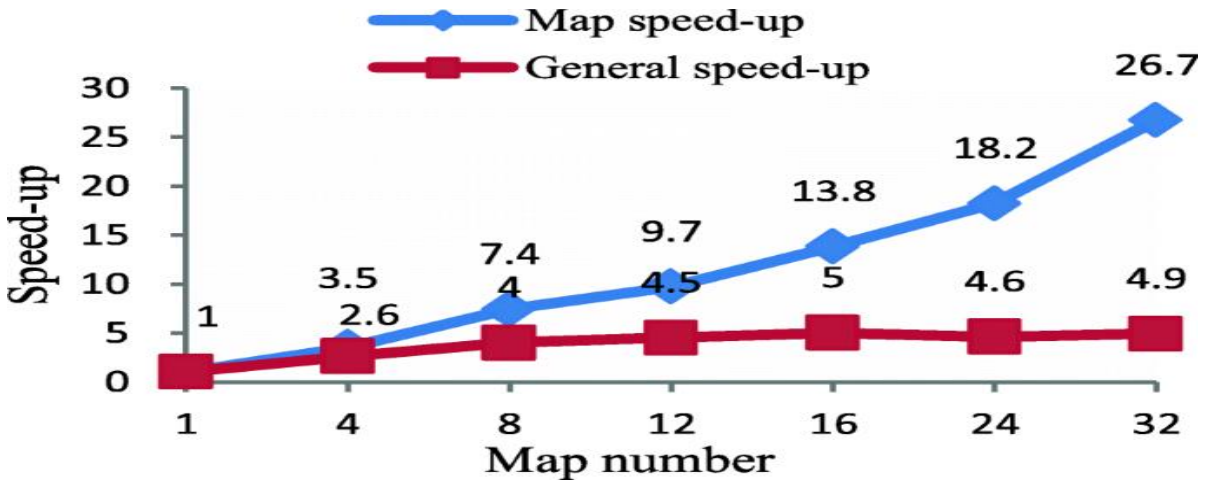

Figure 4. Privacy Protection-Oriented Fully Encrypted Algorithm in Cloud Computing

Fig 4 depicts the privacy protection of fully encrypted algorithms oriented in cloud computing with data security realized within the phases in medical analysis different test patterns are taken into consideration for security in each virtual machine. Cloud instances, available resources, storage attributes, and load balancing may be used to create the goal function of the resource allocation issue. It's also important to keep track of the current condition of server resources in real-time scheduling. This resource allocation system relies heavily on monitoring and resource discovery methods. In the multi-access cloud data security framework, a hybrid multi-access key based data encryption and decryption model is implemented on the large machine learning medical patterns for data recovery and security process.

5. Conclusion

In this work, a hybrid Uncertain data integrity and encryption model is designed and implemented on the machine learning medical patterns for strong data security in the cloud computing environment. Since, most of the conventional method use static cloud encryption and decryption algorithm after uploading into the cloud server, it is difficult to recover and provide security before uploading to the different virtual machines. This work is implemented in two phase's i.e data replication phase and multi-user data access security phase. Initially, machine decision patterns are replicated among the multiple servers for data recovering phase. In the multi-access cloud data security framework, a hybrid multi-access key based data encryption and decryption model is implemented on the large machine learning medical patterns for data recovery and security process. Experimental results proved that the present two-phase Uncertain data recovering, and security framework has better computational efficiency than the conventional approaches on large medical decision patterns. In future work, this work will be extended to implement parallel processing using Hadoop framework due to high dimensional medical patterns in the distributed way.

References

[1] Ahamad, D., Hameed, S. A., & Akhtar, M. (2020). A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. Journal of King Saud University-Computer and Information Sciences.

[2] Xu, Z., He, D., Wang, H., Vijayakumar, P., & Choo, K. K. R. (2020). A novel proxy-oriented public auditing scheme for cloud-based medical cyber physical systems. Journal of information security and applications, 51, 102453.
[3] Ganapathy, S. (2019). A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Computer Networks, 151, 181-190.
[4] Sarosh, P., Parah, S. A., Bhat, G. M., & Muhammad, K. (2021). A security management framework for big data in smart healthcare. Big Data Research, 25, 100225.
[5] Vengadapurvaja, A. M., Nisha, G., Aarthy, R., & Sasikaladevi, N. (2017). An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia computer science, 115, 643-650.
[6] Thirumalai, C., Mohan, S., & Srivastava, G. (2020). An efficient public key secure scheme for cloud and IoT security. Computer Communications, 150, 634-643.
[7] Benil, T., & Jasper, J. J. C. N. (2020). Cloud based security on outsourcing using blockchain in E-health systems. Computer Networks, 178, 107344.
[8] Carter, A. B. (2019). Considerations for genomic data privacy and security when working in the cloud. The Journal of Molecular Diagnostics, 21(4), 542-552.
[9] Sharma, G., Bousdras, G., Ellinidou, S., Markowitch, O., Dricot, J. M., & Milojevic, D. (2021). Exploring the security landscape: NoC-based MPSoC to Cloud-of-Chips. Microprocessors and Microsystems, 84, 103963.
[10] Blanquer, I., Brasileiro, F., Brito, A., Calatrava, A., Carvalho, A., Fetzer, C., ... & Silva, F. (2020). Federated and secure cloud services for building medical image classifiers on an intercontinental infrastructure. Future Generation Computer Systems, 110, 119-134.
[11] Gill, K. S., Saxena, S., & Sharma, A. (2020). GTM-CSec: game theoretic model for cloud security based on IDS and honeypot. Computers & Security, 92, 101732.
[12] Garg, D., Sidhu, J., & Rani, S. (2019). Improved TOPSIS: A multi-criteria decision making for research productivity in cloud security. Computer Standards & Interfaces, 65, 61-78.
[13] Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems, 80, 103301.
[14] Gudditti, V., & Krishna, P. V. (2021). Light weight encryption model for map reduce layer to preserve security in the big data and cloud. Materials Today: Proceedings.
[15] Ayub, M. F., Mahmood, K., Kumari, S., & Sangaiah, A. K. (2021). Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. Digital Communications and Networks, 7(2), 235-244.
[16] Zhou, L., Fu, A., Mu, Y., Wang, H., Yu, S., & Sun, Y. (2021). Multicopy provable data possession scheme supporting data dynamics for cloud-based electronic medical record system. Information Sciences, 545, 254-276.
[17] Jayaram, R., & Prabakaran, S. (2021). Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. Egyptian Informatics Journal, 22(4), 401-410.
[18] Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 33(7), 810-819.
[19] Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97-108.
[20] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642.
[21] Marwan, M., Kartit, A., & Ouahmane, H. (2018). Security enhancement in healthcare cloud using machine learning. Procedia Computer Science, 127, 388-397.

[22] Sri[1], V. D. S., & Vemuru, S. (2019). SURVEY ON DATA SECURITY ISSUES RELATED TO MULTI-USER ENVIRONMENT IN CLOUD COMPUTING. Journal of Critical Reviews, 7(4), 2020.

[23] Mostafa, A. M., & Youssef, A. E. (2013, April). A multi-primary ownership partitioning protocol for highly scalable and available replication services. In 2013 Saudi International Electronics, Communications and Photonics Conference (pp. 1-5). IEEE.

[24] Stiemer, A., Fetai, I., & Schuldt, H. (2016, December). Analyzing the performance of data replication and data partitioning in the cloud: The BEOWULF approach. In 2016 IEEE international conference on big data (Big Data) (pp. 2837-2846). IEEE.

[25] Patel, K., Singh, N., Parikh, K., Kumar, K. S., & Jaisankar, N. (2014, February). Data security and privacy using data partition and centric key management in cloud. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE.

[26] El-Shamy, A. M., El-Fishawy, N. A., Attiya, G., & Mohamed, M. A. (2021). Anomaly detection and bottleneck identification of the distributed application in cloud data center using software–defined networking. Egyptian Informatics Journal, 22(4), 417-432.

[27] El-Shamy, A. M., El-Fishawy, N. A., Attiya, G., & Mohamed, M. A. (2021). Anomaly detection and bottleneck identification of the distributed application in cloud data center using software–defined networking. Egyptian Informatics Journal, 22(4), 417-432.