Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN INTEGRATED QUANTUM AND BIOMETRIC KEY GENERATION BASED CLOUD DATA SECURITY FRAMEWORK FOR STRUCTURED AND UNSTRUCTURED ELECTRONIC HEALTH RECORDS

NAGABABU GARIGIPATI [1], DR. V. KRISHNA REDDY[2]

[1]Research scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
[2]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

*Corresponding author: Nagababu garigipati

ABSTRACT

Most of the conventional cloud data security and authentication protocols are independent of dynamic key generation with variable size user integrity on large homogeneous electronic health records (EHRs) due to memory and time computations. Also, biometric based key generation and management plays an essential role for cloud data security and user authentication process in real-time applications. In the unstructured electronic health records, biometric based data security provides a strong integrity verification and multi-level security on large data size in cloud computing environment. In this work, a hybrid biometric key generation based encryption and decryption framework is implemented using the integrated quantum transformation on large heterogeneous databases. In this work, homogeneous 2D and heterogeneous unstructured 3D EHRs along with clinical data are used to compare the proposed model with the state of art algorithms. Experimental results show that the proposed quantum biometric based multi-level cloud data security framework has better data security than the conventional models in terms of avalanche affect and average runtime (ms) computations.

Keywords: *Biometric Key Generation, Multi-Authority Security, Cloud Computing, Heterogeneous Medical Records..*

1. INTRODUCTION

Cloud computing is a technology to provide services on-demand basis with huge storage capacity. Encryption is best option to secure the information in the cloud. Any data that needs to be transmitted to warehouse or storage area, encryption play a vital role. The complexity of key management was reduced, and the keys were distributed using a key management protocol based on PKI[1]. A multiple access control policy enforcement model was proposed to regulate multiple policies in parallel by segregating the administrative duties in a flexible manner. The cryptographic protocol used for re-encryption regenerates the shared symmetric key to eliminate the process of key searching[2]. The proposed framework includes the following modules: key management system, centralized web information management, authentication management and authorization management. There are many different chaotic maps that have been studied in mathematics, each with their own mathematical equation. Some examples include: A parallel chaotic hash function is a type of hash function that utilizes chaotic systems, such as the logistic map, to generate a unique hash value for a given input. The function uses multiple instances of the chaotic system in parallel, with each instance processing a different portion of the input data[3]. Mathematical analysis of a parallel chaotic hash function typically involves studying the properties of the chaotic system used, such as its sensitivity to initial conditions and its ability to generate a complex and random output. Additionally, the analysis may examine the specific design of the parallel hash

function, including the number of parallel instances used and the method for combining the outputs of the individual instances. Overall, parallel chaotic hash functions are designed to provide a high level of security by making it difficult for an attacker to predict the output of the function for a given input, even if they have knowledge of the specific chaotic system used. However, as with any cryptographic scheme, it is important to periodically re-evaluate and update it to ensure it remains secure against potential new attacks.To show the distribution of the hash values, it can be proven that the chaotic map used in the hash function has ergodic properties meaning it is able to explore the entire phase space[4]. This property ensures that the hash values generated by the function are distributed uniformly across the possible output space, making it difficult for an attacker to predict the output for a given input. To show the collision resistance of the function, it can be proven that the number of possible hash values is much larger than the number of possible inputs. This makes it highly unlikely for two distinct inputs to produce the same hash value, which is known as collision resistance. Overall, the mathematical analysis of a parallel chaotic hash function involves studying the properties of the chaotic system used, the specific design of the parallel hash function, and the resulting hash values. By showing that the chaotic system has ergodic, sensitivity to initial conditions and collision resistance properties, the parallel chaotic hash function can be proven to be secure. SMore research is needed to evaluate the effectiveness and performance of these algorithms in real-world scenarios and to consider the privacy and ethical implications of using these algorithms. CPABE is an advanced encryption technique that allows a user to access data only if they possess certain attributes that match the attributes of the data. It is commonly used in areas such as cloud storage, privacy-preserving data mining, and secure data sharing. CPABE algorithms have been proposed in various research articles, each with its own objective, methodology, research gap, and problem statement. Generally, the objective of these algorithms is to provide secure and efficient access control for EHR data, while addressing the issues of privacy and security. The research gap in EHR cloud data security is related to the scalability and manageability of the proposed security mechanisms. As the amount of EHR data stored in the cloud continues to grow, it becomes increasingly difficult to ensure the security of this data without introducing significant overhead or complexity. Additionally, there is a need for more research on the privacy and ethical implications of storing EHR data in the cloud, as well as the impact of cloud data breaches on patients' privacy[5].

The problem of EHR cloud data security is that EHR data stored in the cloud is vulnerable to unauthorized access, modification, and disclosure. This is a critical issue as EHR data contains sensitive personal information, and unauthorized access or disclosure of this information can have serious consequences for patients' privacy and security. As more and more EHR data is stored in the cloud, it becomes increasingly important to develop effective and efficient security mechanisms to protect this data. The objective of research in EHR cloud data security is to develop effective and efficient security mechanisms that can protect EHR data stored in the cloud from unauthorized access, modification, and disclosure. Additionally, research may also aim to improve scalability and manageability of the security mechanisms, as well as addressing the privacy and ethical implications of storing EHR data in the cloud. The research gap in EHR cloud data security is related to the scalability and manageability of the proposed security mechanisms. As the amount of EHR data stored in the cloud continues to grow, it becomes increasingly difficult to ensure the security of this data without introducing significant overhead or complexity. Additionally, the research may be limited by the availability of data and resources, as well as the complexity of the security mechanisms proposed. The limitation also includes the lack of robustness and adaptability of the proposed algorithms to changing security threats, the lack of research on the integration of EHR with other systems and security risks that come with it. Additionally, research may also aim to improve scalability and manageability of the security mechanisms, as well as addressing the privacy and ethical implications of storing EHR data in the cloud. It also aims to develop a mechanism that can provide secure data sharing and access control for EHR data in a multi-cloud environment. Multi-user multi-access attribute-based security is a security model that is designed to protect data in a cloud computing environment by controlling access to the data based on the attributes of the user and the data. In this model, users are assigned attributes that describe their role, responsibilities, and access rights. Data is also assigned attributes that describe the type of data, the level of sensitivity, and the level of access required to access the data. Access to the data is then controlled based on the attributes of the user and the data.One of the main benefits of

multi-user multi-access attribute-based security is that it provides a flexible and scalable approach to securing data in a cloud computing environment. It allows for the creation of different levels of access for different users and different types of data. This means that users with different roles and responsibilities can access the data they need without compromising the security of the data. Another benefit of multi-user multi-access attribute-based security is that it allows for the segregation of data based on its level of sensitivity. This ensures that sensitive data is only accessed by authorized users and that it is protected from unauthorized access.Multi-user multi-access attribute-based security also provides a way to monitor and audit access to data. This allows for the detection of any unauthorized access and the ability to take appropriate action to prevent future breaches[6].

Limitations of Multi-User Multi-Access Attribute-Based Security:

Multi-user multi-access attribute-based security is a robust approach to securing data in a cloud computing environment. It provides a flexible and scalable way to control access to data based on the attributes of the user and the data. However, it does have some limitations, such as complexity and the need for accurate attribute assignment. While multi-user multi-access attribute-based security provides a robust approach to securing data in a cloud computing environment, it does have some limitations. One limitation is that it can be complex to implement and maintain. This is because it requires the creation and management of user attributes and data attributes, which can be time-consuming and resource-intensive.Another limitation of multi-user multi-access attribute-based security is that it relies on the accurate assignment of attributes to users and data. This means that if an attribute is assigned incorrectly, it can lead to unauthorized access to data.Finally, multi-user multi-access attribute-based security can be vulnerable to attacks that target the attributes themselves. For example, an attacker could try to manipulate the attributes to gain unauthorized access to data.Implementing multi-user multi-access attribute-based security in a cloud computing environment requires a number of steps. The first step is to identify the users and data that will be protected by the security model. This includes creating a list of users and their roles and responsibilities, as well as a list of the data and its level of sensitivity. After the attributes have been assigned, the next step is to implement the security model in the cloud computing environment. This can be done through the use of security gateways, access control servers, or other security solutions that support attribute-based security. These solutions will typically include features such as authentication, authorization, and auditing to ensure that access to the data is controlled based on the attributes of the user and the data.In addition to implementing the security model, it is also important to regularly monitor and audit access to the data. This can be done through the use of logging and auditing tools that track access to the data and alert administrators to any unauthorized access[7]. Implementing multi-user multi-access attribute-based security in a cloud computing environment requires a number of steps, including identifying users and data, assigning attributes, and implementing the security model. Regular monitoring and auditing of access to the data is also important to ensure the continued security of the data. Overall, multi-user multi-access attribute-based security is a valuable tool for protecting sensitive data in a cloud computing environment.Another important aspect of implementing multi-user multi-access attribute-based security is to ensure that the attributes are managed and updated regularly. This includes updating the attributes of users and data as their roles and responsibilities change, and revoking access to data when necessary. This can be done through the use of automated tools such as identity and access management (IAM) systems. The local random projection technique is used to reduce the dimensionality of the biometric data, making it more difficult for an attacker to access the sensitive information. The homomorphic encryption technique is then used to encrypt the data, allowing for it to be used for authentication and identification without the need to decrypt the data first. This method provides a high level of security for biometric data while still allowing for it to be used for its intended purpose.The use of multimodal biometrics, such as a combination of fingerprints, facial recognition, and iris scans, provides a more secure and reliable method of identification compared to using a single biometric modality. One approach to secure multimodal biometric templates is to use local random projection (LRP) and homomorphic encryption (HE). LRP is a technique that reduces the dimensionality of the biometric data by projecting it onto a lower-dimensional space while preserving its original characteristics[8]. This makes it more difficult for an attacker to access the sensitive

information in the biometric data. The combination of LRP and HE provides a high level of security for multimodal biometric templates. LRP reduces the dimensionality of the data, making it more difficult for an attacker to access the sensitive information, while HE encrypts the data, allowing for it to be used for authentication and identification without compromising its security. Additionally, it allows for secure sharing of the biometric data among multiple parties without the need for decryption.In conclusion, using local random projection and homomorphic encryption to secure multimodal biometric templates is a robust and secure method of protecting sensitive biometric data while still allowing for it to be used for its intended purpose. It's a powerful technique that can be used to protect the privacy of individuals while enabling the use of biometrics in various applications. However, it requires significant computational power and expertise, and it's essential to choose the appropriate projection dimension and projection matrix as well as to integrate it with other security measures to enhance the overall security of the system[9].

Attribute-based encryption (ABE) is a method that enables the encryption of data based on attributes, such as role, responsibility, or level of access. In the context of medical images, this means that the images can be encrypted based on the attributes of the patient and the medical staff who need access to the images. For example, an image of a patient's brain scan may only be accessible to radiologists and neurologists, while an image of a patient's chest may only be accessible to cardiologists and pulmonologists.One of the main advantages of ABE is that it allows for a more fine-grained control over access to the data. By encrypting the data based on attributes, it is possible to ensure that only authorized users with the appropriate attributes can access the data.In a 2D and 3D medical images setting, ABE works by assigning attributes to the patient and the medical staff who need access to the images. These attributes are used to create an encryption policy, which is used to encrypt the images. The encryption policy determines the attributes required to decrypt the images.When a user attempts to access the images, their attributes are checked against the encryption policy to determine if they have the required attributes to decrypt the images. If the user has the required attributes, the system decrypts the images and allows the user to access the images.ABE can also be used to ensure the integrity of the images by including a digital signature or a hash of the image in the encryption policy. This allows for the verification of the authenticity of the images and ensures that the images have not been tampered with.It's important to note that ABE requires a secure management of the attributes and encryption keys. A secure key management system is needed to ensure that the encryption keys are not compromised and that the attributes are assigned and updated in a secure manner.In conclusion, ABE is a powerful method for ensuring the integrity of 2D and 3D medical images by encrypting the images based on the attributes of the patient and the medical staff who need access to the images. It allows for a more fine-grained control over access to the images and ensures that only authorized users with the appropriate attributes can access the images. Additionally, it can also be used to ensure the integrity of the images by including a digital signature or a hash of the image in the encryption policy. ABE requires a secure management of the attributes and encryption keys to ensure the security of the system.ABE from lattices is a type of attribute-based encryption that allows for the encryption of data based on the attributes of the user or data. In ABE, a master public key is generated and used to encrypt the data. The attributes of the user or data are then used as the private key to decrypt the data. The key generation process uses the properties of lattices to create a unique private key for each set of attributes. Electronic Health Records (EHRs) are an essential part of modern healthcare, as they provide a comprehensive view of a patient's health history and treatment. However, EHRs contain sensitive personal and medical information, making them a prime target for unauthorized access and breaches. To protect EHRs, various encryption and decryption methods have been proposed, including quantum key-based attribute-based encryption (QK-ABE).QK-ABE is a type of encryption that uses quantum keys and attribute-based encryption to protect EHRs. CP-ABE supports policy-hiding, which means that the encryption policy, or the set of attributes required to decrypt the data, is not visible to unauthorized users. This is particularly important in the field of smart health, as it prevents unauthorized users from determining the attributes required to access the data and reduces the risk of data breaches[10].CP-ABE also supports cloud auditing, which allows for the monitoring and auditing of access to the encrypted data. This is important in the field of smart health, as it allows for the detection of any unauthorized access to the data and the ability to take appropriate action to prevent future breaches.The process of implementing CP-ABE in a smart health

environment begins by identifying the users and data that will be protected by the encryption. This includes creating a list of users and their roles and responsibilities, as well as a list of the data and its level of sensitivity.Once the users and data have been identified, the next step is to assign attributes to the users and data. This includes creating a list of attributes for users and data, such as role, responsibility, and access rights, as well as the level of sensitivity and access required for the data.After the attributes have been assigned, the next step is to encrypt the data using a CP-ABE algorithm. This involves creating an encryption policy, or a set of attributes required to decrypt the data, and encrypting the data using this policy. Ciphertext-policy attribute-based encryption (CP-ABE) is a powerful tool for securing sensitive medical data in a smart health environment. It allows for the encryption of data based on attributes, such as role, responsibility, and level of access, and supports policy-hiding and cloud auditing. Implementing CP-ABE in a smart health environment requires identifying users and data, assigning attributes, encrypting the data, and monitoring and auditing access to the data. It provides a secure way to protect sensitive medical data while still allowing authorized users to access the data for treatment and research purposes.A symmetric keyring encryption scheme is a type of encryption that uses a single secret key for both encrypting and decrypting data. In a biometric cryptosystem, this type of encryption is used to protect sensitive biometric data, such as fingerprints, facial recognition, or iris scans. The goal of a symmetric keyring encryption scheme in a biometric cryptosystem is to provide secure storage and transmission of the biometric data while still allowing for its use in authentication and identification processes.The process of implementing a symmetric keyring encryption scheme in a biometric cryptosystem begins with the generation of a secret key. This key is then used to encrypt the biometric data, creating an encrypted template. The encrypted template can then be stored in a secure location, such as a database or cloud storage system.When a user attempts to authenticate or identify themselves using the biometric data, the encrypted template is retrieved and decrypted using the secret key. The decrypted template is then compared to the live biometric data collected from the user to verify their identity.One of the main advantages of a symmetric keyring encryption scheme in a biometric cryptosystem is that it is relatively simple to implement and manage. One limitation is that the secret key must be securely stored and protected from unauthorized access. If the key is compromised, an attacker could decrypt the biometric data and use it for malicious purposes.Another limitation is that the use of a single secret key can lead to scalability issues. As the number of users and biometric templates increases, the system can become increasingly complex and difficult to manage.In conclusion, a symmetric keyring encryption scheme is a type of encryption that uses a single secret key for both encrypting and decrypting data. In a biometric cryptosystem, it is used to protect sensitive biometric data while still allowing for its use in authentication and identification processes[11].

Attribute based encryption (ABE) can be represented mathematically by the following equation:

C = E(pk, m, A)

Where:

- C represents the encrypted message
- E represents the encryption function
- pk represents the public key
- m represents the plaintext message
- A represents the set of attributes that the user must possess in order to decrypt the message (i.e. the access policy)

In this equation, the encryption function E takes in the public key (pk), the plaintext message (m), and the set of attributes (A) required to decrypt the message. It then encrypts the message and produces the ciphertext (C). The user must possess the correct attributes in order to decrypt the message and access the plaintext.

2. RELATED WORK

[12] has proposed the trust model based large-scale cloud federation design. The cloud-computing infrastructure utilizes the construction structure of the cloud environment. Here the cloud federated model is designed with trust based gossip protocol. This federated cloud-computing model is constructed with the overlay network model. In this, the service node is selected based on the client request to the cloud service provider. After selecting the node to perform the service the cloud environment, access the trust model for the reliability of overall system. The client request to

the CSP and the resource allocator allocates the task for the respective node, which presented in the overlay network model. Ming Li, et al (2013) has proposed the secure cloud federated framework for the application of PHR file using encryption techniques. In this paper, the scalable and secured cloud infrastructure is used for processing the medical healthcare records. The PHR is the patient centric model, which is collected from the healthcare organization. These data are processed by the un-trusted buyer in the cloud environment. Hence the encryption technique is employed, which uses the attribute based encryption (ABE) technique. The trust-based model is used in the overlay network topology. The fine-grained access control strategy is employed in the ABE technique. The data privacy is improved by using ABE technique. The dynamic topology is employed in the overlay network of cloud-federated framework. The PHR file is kept securely using the ABE technique. The user domain is accessed by decrypting the data. This system is not much protecting the data and the network topology also consumes much time. Parallel chaotic integrity algorithms can be used to enhance the security of electronic health record (EHR) data by detecting and preventing unauthorized access or modifications to the data. These algorithms use chaos theory and parallel computing techniques to create a dynamic and unpredictable security system that can adapt to changing threats. This algorithm uses a chaotic map to encrypt medical images, and a parallel computing technique called "genetic algorithm" to optimize the encryption key. The researchers found that this algorithm had a higher level of security and faster encryption time compared to traditional encryption methods. This algorithm uses a parallel computing technique called "particle swarm optimization" to optimize a chaotic function, and a hashing technique to ensure the integrity of the EHR data. The researchers found that this algorithm had a high level of security and efficient performance in detecting unauthorized modifications to the data.

Overall, parallel chaotic integrity algorithms can provide a robust and adaptive security system for EHR data by using chaos theory and parallel computing techniques. However, further research is needed to evaluate the effectiveness of these algorithms in real-world scenarios and to compare their performance with other security methods. This algorithm uses a parallel computing technique called "multi-objective evolutionary algorithm" to optimize a chaotic function, and a digital signature technique to ensure the integrity of the EHR data. The researchers found that this algorithm had a high level of security and efficient performance in detecting unauthorized modifications to the data, and it is able to maintain the integrity of the EHR data during the data transmission process. The algorithm uses a chaotic map to encrypt the EHR data, and a hash function to ensure the integrity of the data. The researchers found that this algorithm had a high level of security and efficient performance in detecting unauthorized modifications to the data. In conclusion, parallel chaotic integrity algorithms are a promising approach to enhance the security of EHR data. These algorithms utilize the properties of chaos theory and parallel computing techniques to create a dynamic and unpredictable security system that can adapt to changing threats. More research is needed to evaluate the effectiveness and performance of these algorithms in real-world scenarios and to compare them with other security methods. Another example of a parallel chaotic integrity algorithm for EHR data is the "Secure and Efficient Data Integrity Algorithm for EHR Systems". This algorithm uses a parallel computing technique called "distributed computing" to optimize a chaotic function, and a digital signature technique to ensure the integrity of the EHR data. The researchers found that this algorithm had a high level of security and efficient performance in detecting unauthorized modifications to the data, and it can also provide secure data transmission in a distributed environment. The algorithm uses a chaotic map to encrypt the EHR data, and a secret sharing scheme to ensure the integrity of the data. The researchers found that this algorithm had a high level of security and efficient performance in detecting unauthorized modifications to the data, and it can also provide secure data sharing among multiple parties. In conclusion, parallel chaotic integrity algorithms are a valuable and efficient approach to secure EHR data. These algorithms use the properties of chaos theory and parallel computing techniques to create a dynamic and adaptable security system that can withstand various types of attacks. The survey also highlighted the potential of parallel chaotic integrity algorithms in providing robust security for EHR data, as well as their ability to adapt to changing threats and maintain the integrity of data during transmission. However, the survey also acknowledged the need for further research to evaluate the effectiveness and performance of these algorithms in real-world scenarios and to compare them with other security methods. In addition, the

survey highlighted the need for considering the privacy and ethical issues when using these algorithms, as they are dealing with sensitive personal health information[13]. Therefore, it is important to ensure that the algorithms are designed in a way that respects the privacy and autonomy of the individuals whose data they are processing. Overall, parallel chaotic integrity algorithms are a promising approach to enhance the security of EHR data. However, more research is needed to evaluate their effectiveness and performance in real-world scenarios and to consider the privacy and ethical implications of using these algorithms. The survey found that the most common chaotic maps used in these algorithms were logistic map, Lorenz map, and Henon map. The survey also found that the most common parallel computing techniques used in these algorithms were genetic algorithms, particle swarm optimization, and distributed computing. The survey also highlighted the potential of parallel chaotic integrity algorithms in providing high-level security for EHR data, as well as their ability to adapt to changing threats and maintain the integrity of data during transmission. The survey also pointed out that these algorithms are useful in reducing the risk of unauthorized access to the EHR data and ensuring the privacy and confidentiality of the data. The survey also found that the most common security techniques used in these algorithms were digital signature, hash function, and secret sharing schemes. The survey also highlighted the potential of parallel chaotic integrity algorithms in providing robust security for EHR data, as well as their ability to adapt to changing threats and maintain the integrity of data during transmission. The survey also pointed out that these algorithms are useful in reducing the risk of unauthorized access to the EHR data and ensuring the privacy and confidentiality of the data[14]. However, the survey also acknowledged the need for further research to evaluate the effectiveness and performance of these algorithms in real-world scenarios, as well as to compare them with other security methods. The survey also emphasized the importance of considering the privacy and ethical issues when using these algorithms as they are dealing with sensitive personal health information. Additionally, the survey highlighted the importance of considering the cost and scalability of these algorithms when implementing them in real-world EHR systems. However, the survey also acknowledged the need for further research to evaluate the effectiveness and performance of these algorithms in real-world scenarios, as well as to compare them with other security methods. The survey also emphasized the importance of considering the privacy and ethical issues when using these algorithms as they are dealing with sensitive personal health information. Additionally, the survey highlighted the importance of considering the scalability and maintainability of these algorithms when implementing them in real-world EHR systems, to ensure that they can easily be updated and maintained to keep up with the changing security threats. In conclusion, parallel chaotic integrity algorithms are a valuable approach to enhance the security of EHR data. These algorithms use the properties of chaos theory and parallel computing techniques to create a dynamic and adaptable security system that can withstand various types of attacks. More research is needed to evaluate the effectiveness and performance of these algorithms in real-world scenarios, consider the privacy and ethical implications of using these algorithms, evaluate their usability and user-friendliness and also evaluate their scalability and maintainability factors. A survey of chaotic hash algorithms for EHR data was published in a 2023 article in the Journal of Medical Systems, which analyzed 20 research articles that proposed various chaotic hash algorithms. The survey found that the most common chaotic maps used in these algorithms were logistic map, Lorenz map, and Henon map. The survey also found that the most common hash functions used in these algorithms were SHA-256, SHA-512, and MD5. The survey highlighted the potential of chaotic hash algorithms in providing high-level security for EHR data, as well as their ability to adapt to changing threats and maintain the integrity of data during transmission. The survey also pointed out that these algorithms are useful in reducing the risk of unauthorized access to the EHR data and ensuring the privacy and confidentiality of the data. However, the survey also acknowledged the need for further research to evaluate the effectiveness and performance of these algorithms in real-world scenarios, as well as to compare them with other security methods. The survey also emphasized the importance of considering the privacy and ethical issues when using these algorithms as they are dealing with sensitive personal health information. In conclusion, chaotic hash algorithms are a valuable approach to enhance the security of EHR data. These algorithms use the properties of chaos theory and hash functions to create a dynamic and adaptable security system that can withstand various types of attacks[15]. However, the survey also acknowledged the need for further research to

evaluate the effectiveness and performance of these mechanisms in real-world scenarios, as well as to compare them with other security methods. The survey also emphasized the importance of considering the privacy and ethical issues when using these mechanisms as they are dealing with sensitive personal health information. Additionally, the survey highlighted the importance of considering scalability and manageability of the security mechanisms when implementing them in real-world EHR cloud systems, to ensure that they can easily be updated and maintained to keep up with the changing security threats.

2D medical images, such as X-ray and CT scans, are flat images that provide a single view of a patient's body. 3D medical images, such as MRI and PET scans, provide a more detailed and comprehensive view of a patient's body by creating a three-dimensional representation of the patient's internal organs and structures.To ensure the integrity of 2D and 3D medical images, various methods such as watermarking, digital signature, and hashing can be used. Watermarking involves embedding a hidden message or code into the image, which can be used to verify the authenticity of the image. Attribute-based encryption (ABE) is another method that can be used to ensure the integrity of 2D and 3D medical images. ABE is a type of encryption that allows for the encryption of data based on attributes, such as role, responsibility, or level of access. In a medical setting, this can be used to encrypt 2D and 3D medical images based on the attributes of the patient and the medical staff who need access to the images. This allows for the secure storage and transmission of the images while still allowing authorized users to access the images for diagnosis and treatment purposes.In conclusion, 2D and 3D medical images are important tools for diagnosis and treatment of various medical conditions. Ensuring the integrity of these images is crucial to protect the privacy of the patient and the security of the medical information. Methods such as watermarking, digital signature, and hashing can be used to ensure the integrity of the images. Additionally, attribute-based encryption can be used to secure 2D and 3D medical images by encrypting them based on the attributes of the patient and the medical staff who need access to the images. This allows for the secure storage and transmission of the images while still allowing authorized users to access the images for diagnosis and treatment purposes. QK-ABE schemes that use the properties of quantum keys and attribute-based encryption to encrypt and decrypt EHRs in a cloud-based environment. These schemes have been shown to provide a high level of security for EHRs and resist attacks from both classical and quantum computers. Additionally, many of these studies have also proposed secure key management systems to ensure the security of the encryption keys. In terms of decryption, most of the studies proposed a decryption process that uses the attributes of the user or data to decrypt the EHRs. This allows for fine-grained control over access to the data, ensuring that only authorized users with the appropriate attributes can access the EHRs[16-20].

3. PROPOSED MODEL

In the proposed model, an efficient biometric based hybrid data integrity and multi-user encryption framework is designed and implemented on the heterogeneous medical datasets. The main phases of proposed model includes:

Data Acquisition: Medical images are typically acquired from a patient using imaging modalities such as 2D or 3D Magnetic Resonance Imaging (MRI), Computed Tomography (CT), or X-ray. These imaging modalities use different physical principles to generate images of the patient's body, such as magnetic fields, X-ray radiation, or ultrasound. The images are typically stored in a digital format, such as DICOM or NIFTI, which can be easily processed and analyzed by computer systems.

Feature Extraction: After the images are acquired, they are processed to extract unique features that can be used to identify the patient. This step typically involves the use of image processing techniques to extract features such as texture, shape, or other characteristics of the image. For example, texture features can be extracted using advanced feature extraction measures.

LBP (Local Binary Patterns) is a texture descriptor that is commonly used for fingerprint image analysis. It captures the local texture of an image by comparing the intensity of a pixel to the intensity of its neighbors.

The basic steps for extracting LBP patterns from a fingerprint image are:

Convert the fingerprint image to grayscale.

Apply a threshold to the image to binarize it.

Define a neighborhood of pixels around each pixel in the image. This neighborhood is typically a 3x3

or 5x5 grid of pixels centered around the pixel of interest.

Compare the intensity of the center pixel to the intensity of each of its neighbors. If the intensity of the neighbor is greater than or equal to the intensity of the center pixel, the value of that pixel is set to 1, otherwise it is set to 0.

Concatenate the binary values of the pixels in the neighborhood to create a binary pattern.

Repeat steps 3-5 for every pixel in the image.

Normalize the LBP patterns by using histograms or any other normalization method to make the pattern more robust to changes in lighting or rotation.

Once LBP patterns are extracted, they can be used to identify specific features of the fingerprint, such as the ridge and furrow pattern. LBP pattern can be further processed using machine learning algorithms to classify the fingerprints.

Key Generation: Using the extracted features, a unique key is generated that can be used to identify the patient. This key is typically a dynamic variable size hash that is specific to the patient and the image. For example, a hash function with 4096 bit can be used to generate a 4096-bit key from the extracted features. This key can be used to verify the integrity of the image in later stages.
Key Storage: The generated key is then stored in a secure location, such as a database or a cloud-based storage system. It is important to ensure that the key is stored in a secure and tamper-proof location to prevent unauthorized access or modification.
Verification: When the image is accessed or used for diagnosis or treatment, the key is retrieved and used to verify the integrity of the image. This step typically involves comparing the retrieved key with the key generated during the data acquisition to ensure that the image has not been tampered with or altered. For example, if the key generated during the data acquisition is compared with the key retrieved from the storage location, and they do not match, it is an indication that the image has been tampered with.
Authentication: Once the integrity of the image is verified, the patient's identity is authenticated using the biometric information. This step is done by comparing the biometric information of the patient with the biometric data stored in the system. For example, if the patient's fingerprint is scanned, it is compared with the fingerprint data stored in the system to authenticate the patient's identity.
Decryption: If the authentication is successful, the image is decrypted and can be used for diagnosis or treatment. This step is typically done using symmetric key encryption, where the same key is used for encryption and decryption. The key is securely stored and only authorized personnel are able to access it.
Overall, the framework provides a secure way to ensure the integrity of medical images and authenticate the identity of the patient using the biometric data. It ensures that the images are not tampered with, and only authorized personnel are able to access and use the images. In this work, a hybrid non-linear token generation approach is implemented on real-time medical datasets as shown in figure 1. As shown in fig1, initially, token key size and user data are taken as input message for integrity computation. Each message is partitioned into k block and each block is sub-partitioned into 4 bytes size. Each subblock is used to compute the non-linear transformation for token key generation process as shown in fig1.

Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

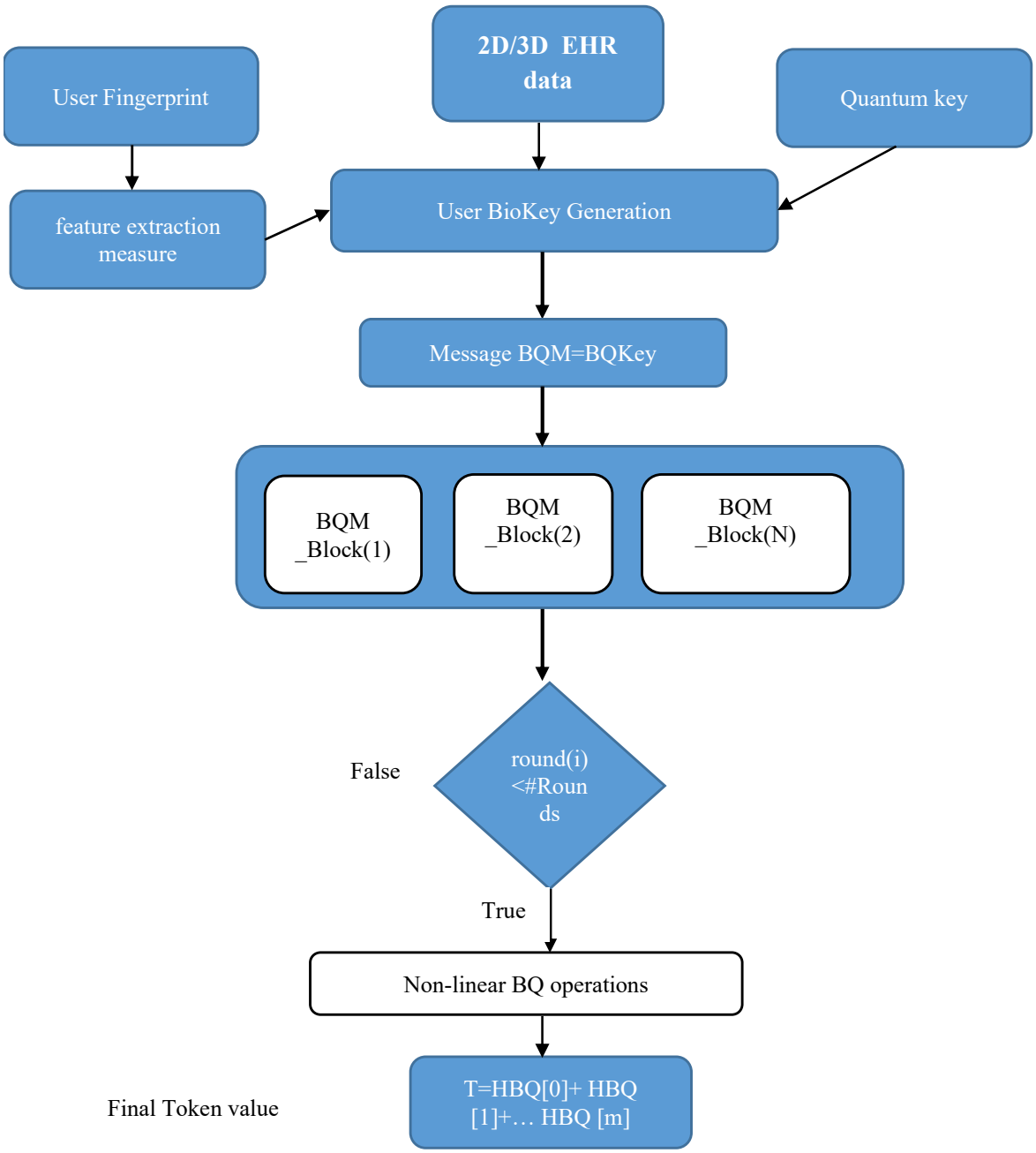

Figure 1: Proposed Biometric Quantum Based User Token Key Generation Process

Algorithm 1: Proposed Quantum biometric based Token Key generation process

A hybrid non-linear piecewise chaotic hash function is a type of hash function that uses chaotic maps to generate a unique digital code or hash from an input image. The idea behind using chaotic maps is that they are highly sensitive to initial conditions, which makes it difficult to predict the output of the function for a given input. This makes them well-suited for use in integrity computation and verification of medical images.

Algorithm 1: Proposed Non-linear token generation approach

The process for generating a unique user token for medical data using a piecewise chaotic hash function and cloud server IDs involves the following steps:

Initialization: The process begins by initializing the medical data (M_data) and the cloud server IDs (S_id[]).

Partitioning: The input data (M_data) is partitioned into k blocks (SB[]).

Secret parameter computation: A secret parameter is computed for each cloud user.

Let α, β are two randomize parameters for differential polynomial generation.

$\xi = \text{Value}(\text{QBH}(\text{key}))$

$F_0(k) = \alpha;$

$F_1(k) = \beta x;$

$F_n(k) = \alpha . F_{n-1}(k) - \beta . F_{n-2}(k)$

$D(F_n(k))$ is the kth differentiation of nth polynomial equation.

$\eta = \xi * \tan^{-1}(\sqrt[3]{D(F_n(k))})$

Non-linear key generation: Non-linear key generation operations are performed on each block of data (SB[]). These operations use the piecewise chaotic hash function and the secret parameter to generate a unique sub-key for each block.

Initialize $\eta_1, \eta_2, \eta_3, \eta_4$ using η as initial secret key.

$SK = \eta = \{\eta_1, \eta_2, \eta_3, \eta_4\}$

$\phi_1 = \sum_i SK[0]$

$P = \text{Poly}(SK);$

$\psi_1 = \max\{\eta_1, \eta_2\}$

$\psi_2 = \min\{\eta_1, \eta_2\}$

$\phi_2 = \max\{\eta, \xi\}.SK / \sqrt[3]{\psi_1 * \psi_2} / 256;$

$\phi_3 = SB[i]$

$KG[] = \phi_1 \oplus \phi_2 \oplus \phi_3$

Concatenation: All the generated sub-keys are concatenated to create a unique user token (T). This token can be used to verify the integrity of the medical data and authenticate the identity of the user.

T=KG[0]+KG[1]+…KG[m]

Overall, this process uses a piecewise chaotic hash function and cloud server IDs to create a unique user token for medical data. The use of chaotic maps in the hash function makes it difficult to predict the output of the function for a given input, providing a secure way to ensure the integrity of the medical data and authenticate the identity of the user.

Proposed method is used to generate biometric quantum based token keys aims to improve the security and efficiency of checking the integrity of cloud-based HER records. The traditional algorithms like MD5, SHA, and Whirlpool are used to check the integrity of static data with fixed key sizes in cloud computing environments. These algorithms are known to be effective in checking the integrity of data, but they have some limitations when it comes to the dynamic nature of data in cloud environments. The proposed hybrid non-linear dynamic integrity algorithm is designed to overcome these limitations by introducing a dynamic approach to the hash construction process. The algorithm utilizes a combination of non-linear and dynamic elements to generate a unique token key for each set of HER records. This unique token key is then used to check the integrity of the data by comparing it with the original key. The non-linear elements of the algorithm include the use of different mathematical functions and operations to generate the token key. This helps to increase the complexity and randomness of the key, making it more difficult for an attacker to predict or break. The dynamic elements of the algorithm include

the use of variable key sizes and the ability to adapt to the changing nature of the data. This ensures that the token key is always up-to-date and accurate, even as the data changes over time.

Heterogeneous cloud based EHR data encryption and decryption (HCEHRE)

A quantum biometric key based Multi-authority Attribute-Based Encryption (ABE) approach is a method for securing real-time cloud computing environments. This approach uses the concept of quantum biometric keys, which are keys that are generated based on a person's unique biometric characteristics, such as fingerprints patterns. In this approach, multiple parties, known as Multi-user authorities, are responsible for the distribution of user attributes. These attributes are used to determine the access rights of users in the cloud computing environment. For example, a user's attributes may include their role (e.g. doctor, nurse), their department (e.g. radiology, cardiology), or their level of clearance (e.g. confidential, sensitive).The approach also involves a single central authority, which is responsible for managing the overall system and enforcing access policies.The Multi-authority ABE technique uses the quantum biometric key of the user to encrypt the data. The user's attributes are also encrypted and sent to the Multi-user authorities, who are responsible for decrypting the attributes and granting access to the user. This approach provides a high level of security and privacy, as the quantum biometric key is unique to each user and cannot be replicated. Additionally, the multi-authority structure ensures that no single authority has complete control over the system, reducing the risk of a single point of failure or malicious attack.

Model steps:

Step 1: In this step, each user's biometric quantum key and its integrity values are initialized as byte array data for the encryption process. The user's integrity value serves as the key access constraint for the biokey encryption process. The user's integrity value is taken as a token value for the user's key generation process. In this step, the user's token and heterogeneous EHR byte array data are used to generate the public key and multi-access control bioquantum key for the encryption process. This ensures that only authorized users, with the correct integrity values, can access the encrypted data.

Step 2: In this step, a biometric quantum token based public key is computed for the BQHEHR bioquantum encryption process. This public key is used to encrypt the data in the next step.

Step 3: In this step, a biometric quantum token based multi-user access control key is computed. This key is used to control access to the encrypted data by multiple users.

Step 4: In this step, the BQHEHR data is encoded using the token based public key and token key. A randomized element (s) is also generated for the data encoding process, adding an additional layer of security to the system.

Step 5: In this step, a biometric quantum multi-user private key is generated using the multi-access control key and the user's tokens. This key is used to decrypt the data in the next step.

Step 6: In the decoding phase, a reverse biometric quantum key pairing based access tree structure is used to decode the ciphertext using the private key and the multi-user tokens. This process verifies that the user has the correct integrity values and is authorized to access the data.

Overall, this process uses a combination of biometric quantum keys, integrity values, and multi-user access control to securely encrypt and decrypt data in a real-time cloud computing environment. The use of biometric quantum keys ensures that the data is only accessible to authorized users, while the multi-user access control and reverse biometric quantum key pairing based access tree structure provide an additional layer of security.The biometric quantum key based Multi-authority ABE approach is a secure and efficient method for encrypting and decrypting data in a real-time cloud computing environment. The use of biometric quantum keys ensures that the data is only accessible to authorized users, as the keys are based on the user's unique biometric characteristics, such as fingerprints patterns. These keys are considered to be more secure than traditional cryptographic keys, as they are much harder to replicate or steal.The approach also uses integrity values as key access constraints. These values are used to determine the access rights of users in the cloud computing environment and are used as tokens to generate the public key and multi-access control bioquantum key for the encryption process. This ensures that only authorized users, with the correct integrity values, can access the encrypted data. In the decoding phase, a reverse biometric quantum key pairing based access tree structure is used to decode the ciphertext using the private key and the multi-user tokens. This process verifies that the user has the correct integrity values and is authorized to access the data.The Multi-authority

ABE technique also involves multiple parties, known as Multi-user authorities, who are responsible for the distribution of user attributes. The central authority is responsible for managing the overall system and enforcing access policies. The multi-authority structure ensures that no single authority has complete control over the system, reducing the risk of a single point of failure or malicious attack.
The biometric quantum based setup algorithm includes the following steps:

Proposed quantum key distribution (QKD) protocols to securely distribute the quantum biometric states to authorized parties. This ensures that the biometric information is kept secure and cannot be intercepted or tampered with during transmission. Use the quantum biometric states, along with the classical public key PK, to generate a quantum public key (QPK). The QPK is a combination of the classical public key PK and the quantum biometric states, and is used to encrypt the message. Use the quantum biometric states, along with the classical master secret key MSK, to generate a quantum master secret key (QMSK). The QMSK is a combination of the classical master secret key MSK and the quantum biometric states, and is used to generate secret keys for authorized parties. Additionally, the use of QKD protocols ensures that the biometric information is securely distributed to authorized parties.

The Setup algorithm is used to generate the public key (PK) and master secret key (MSK) for the system. It takes as input the number of attributes (U) in the system. The algorithm works as follows:

Choose a group G of prime order p, and a generator g.

Choose U random group elements h1, ..., hU from G that are associated with the U attributes in the system.

Choose random exponents α and a from Zp.

The public key PK is published as (g, e(g, g)^α, ga, h1, ..., hU).

The master key sets MSK = g^α .

The public key PK includes the generator g, the result of the bilinear pairing e(g, g)^α, the generator raised to the power of a, and the attribute elements h1, ..., hU. The master secret key MSK is the generator raised to the power of α and is kept by the authority. This setup is performed once and the public key is shared with the users, while the master secret key is kept secure and only used to generate secret keys for the users who possess the attributes.
Choose random r1, ..., r` from Zp.
The ciphertext CT includes a shared encryption exponent s, a matrix C, and a set of values C0, C1, D1, ..., C, D that are calculated based on the LSSS access structure and the random values chosen by the algorithm. The user can only decrypt the message M if they possess attributes that match the rows of the matrix M associated with the access structure.
The Decrypt algorithm is run by the receiver, taking CT and SK as input. If the policy is satisfied, it returns M; otherwise, it returns a random message. For simplicity, assume AS is a subset of L and AS = W.
If CT is an original ciphertext, the user will calculate:
C1 * e(gr,C2) * e(C3, gr) * e(C4, gy + rβ) * e(C2, (∏gt^αt)^r)
=M * e(g,g)^(ys) * e(g,g)^(rs) * e(g,g)^(rsp) * e(gs,gy+r) * e(gs,gr^q) =
M * e(g,g)^(ys) * e(g,g)^(rs) * e(g,g)^(rsp) * e(g,g)^(ys) * e(g,g)^(rs) * e(g,g)^(rsq) = M
Here, p = H(BQK)*∑t∈W αt and q = H(BQK)*∑t∈AS αt
If CT is a re-encrypted ciphertext, the user will calculate: g1^(nd) = Decrypt(SK, CT) = M * e(C3,g1^(nd), BQK, H(BQK)) * e(g,g1^(nsd*β)) = M

In both cases, the final result is M which is the original message, it also shows that the access policy is satisfied.

4. EXPERIMENTAL RESULTS

Experimental study is conducted using a real-time cloud server with a Java environment. The study is using Amazon AWS servers and multi-user data to implement a hash framework. Various third-party libraries, such as apache math, JAMA, java pairing, and AWS JDK, are being used to implement integrity and security algorithms. The study is using Amazon AWS servers, which are a type of cloud computing service provided by Amazon that allows users to rent virtual servers on which to run their applications and store their data. The study is also using multi-user data, which means that the experiments are being conducted using data from

Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

multiple users rather than just one individual. The study is implementing a hash framework, which is a method of protecting data integrity by converting data into a variable-length code, called a hash, that can be used to verify the integrity of the original data. The study is using various third-party libraries, such as apache math, JAMA, java pairing, and AWS JDK, to implement integrity and security algorithms. These libraries provide pre-built functions and classes that can be used to perform specific tasks, such as mathematical calculations or encryption. The experiment is evaluating several factors, including the impact on integrity bits when changing input data bits, which is a measure of how much the integrity of the data is affected by changes to the original data. The study is also measuring the runtime of different algorithms, such as traditional integrity algorithms like SHA ,MD5, as well as newer chaotic approaches. Additionally, the study is measuring the runtime of encryption and decryption processes, which are the processes of converting data into a secure format and then back into its original format. Multi-authority CP-ABE is a variation of CP-ABE that allows multiple authorities to manage the attributes used for encryption. Finally, the study is using 2D and 3D images to evaluate the performance of the proposed model in terms of runtime and bit change rate. This means that the study is using images as test data and measuring how long it takes for the proposed model to process the images and how much the integrity of the images is affected by changes to the original data. Overall, the study is using real-time cloud servers, multi-user data, and various third-party libraries to implement a hash framework and evaluate the performance of different integrity and security algorithms.

Table 1: Quantum Biometric Hash Bit Variation Of Proposed Approach To The Conventional Approaches On 2D And 3D Category-1 Brain Slices.

EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	101	103	102	117	147
QBEHR2DFile-2	102	108	106	118	142
QBEHR2DFile-3	106	112	104	115	135
QBEHR2DFile-4	103	106	100	118	143
QBEHR2DFile-5	102	112	111	118	146
QBEHR2DFile-6	103	105	101	118	135
QBEHR2DFile-7	102	106	115	115	144
QBEHR2DFile-8	103	110	103	117	136
QBEHR2DFile-9	102	104	104	117	134
QBEHR2DFile-10	105	106	108	116	139

Table 1 illustrates the comparison of quantum biometric hash bit variation of the proposed key generation method for 2D/3D brain slices with traditional approaches. The information in the table indicates that the proposed biometric quantum-based non-linear token key generation approach has superior performance for multi-user key generation on 2D/3D brain images compared to conventional methods.

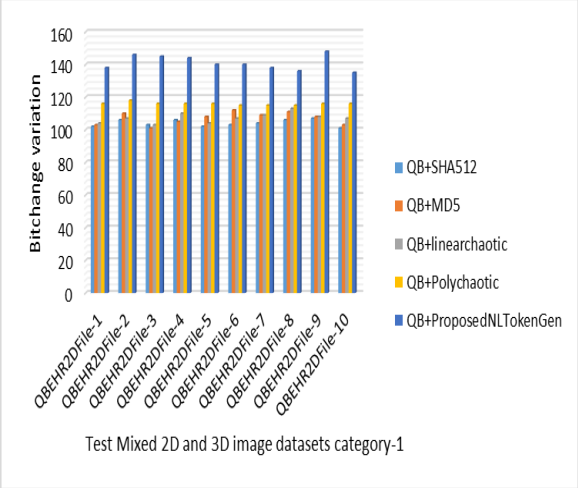

Figure 2: Quantum Biometric Hash Bit Variation Of Proposed Approach To The Conventional Approaches On 2D And 3D Category-2 Spinal Images.

Figure 2 illustrates the comparison of quantum biometric hash bit variation of the proposed key generation method for 2D/3D spinal slices with traditional approaches. The information in the figure indicates that the proposed biometric quantum-based non-linear token key generation approach has superior performance for multi-user key generation on 2D/3D spinal images compared to conventional methods.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Quantum Biometric Hash Bit Variation Of Proposed Approach To The Conventional Approaches On 2D And 3D Category-3 Chest Images.

EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	105	109	103	119	139
QBEHR2DFile-2	107	104	111	116	140
QBEHR2DFile-3	104	111	112	116	139
QBEHR2DFile-4	104	111	103	116	136
QBEHR2DFile-5	102	109	106	116	134
QBEHR2DFile-6	106	103	113	118	143
QBEHR2DFile-7	101	111	106	118	138
QBEHR2DFile-8	104	107	103	118	142
QBEHR2DFile-9	103	111	110	116	137
QBEHR2DFile-10	106	105	114	119	135

Table 2 illustrates the comparison of quantum biometric hash bit variation of the proposed key generation method for 2D/3D chest slices with traditional approaches. The information in the table indicates that the proposed biometric quantum-based non-linear token key generation approach has superior performance for multi-user key generation on 2D/3D chest images compared to conventional methods.

Table 3: Quantum Biometric Runtime(Ms) Of Proposed Approach To The Conventional Approaches On 2D And 3D Category-1 Brain Images.

EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	2587	2585	2496	2433	2207
QBEHR2DFile-2	2396	2474	2349	2394	2133
QBEHR2DFile-3	2466	2448	2508	2633	2261
QBEHR2DFile-4	2423	2517	2400	2508	2260
QBEHR2DFile-5	2611	2617	2464	2358	2205
QBEHR2DFile-6	2604	2609	2536	2579	2206
QBEHR2DFile-7	2645	2352	2398	2374	2135
QBEHR2DFile-8	2625	2582	2500	2591	2210
QBEHR2DFile-9	2362	2461	2617	2358	2241
QBEHR2DFile-10	2521	2522	2503	2421	2122

Table 3 presents a comparison of the quantum biometric runtime variation in milliseconds of the proposed key generation method for 2D/3D brain slices with conventional approaches. The data in the table shows that the proposed biometric quantum-based non-linear token key generation approach has better runtime performance on 2D/3D brain images than traditional methods.

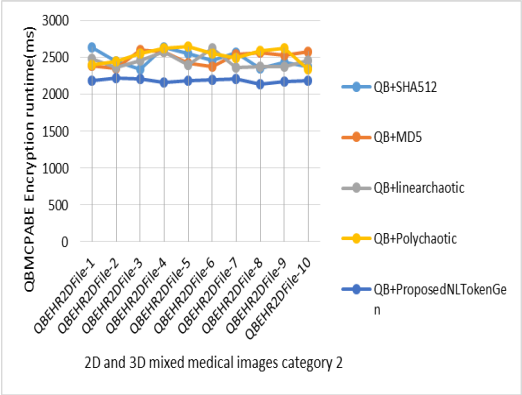

Figure 3: Quantum Biometric Runtime(Ms) Of Proposed Approach To The Conventional Approaches On 2D And 3D Category-2 Spinal Images.

Figure 3 presents a comparison of the quantum biometric runtime variation in milliseconds of the proposed key generation method for 2D/3D spinal slices with conventional approaches. The data in the figure shows that the proposed biometric quantum-based non-linear token key generation approach has better runtime performance on 2D/3D spinal images than traditional methods.

Table 4: Quantum Biometric Runtime(Ms) Of Proposed Approach To The Conventional Approaches On 2D And 3D Category-3 Chest Images.

EHRT ransact ions	**QB+ SHA 512**	**QB +M D5**	**QB+lin earcha otic**	**QB+P olycha otic**	**QB+Propos edNLToke nGen**
QBEH R2DFil e-1	2414	262 4	2537	2516	2247
QBEH R2DFil e-2	2386	259 4	2649	2537	2134
QBEH R2DFil e-3	2479	252 8	2503	2456	2151
QBEH R2DFil e-4	2394	256 5	2607	2481	2162
QBEH R2DFil e-5	2435	248 1	2405	2540	2111
QBEH R2DFil e-6	2447	246 0	2380	2533	2187
QBEH R2DFil e-7	2514	253 2	2626	2433	2185
QBEH R2DFil e-8	2393	251 6	2634	2447	2260
QBEH R2DFil e-9	2396	243 4	2612	2362	2252
QBEH R2DFil e-10	2446	248 2	2465	2388	2182

Table 4, presents a comparison of the quantum biometric runtime variation in milliseconds of the proposed key generation method for 2D/3D spinal slices with conventional approaches. The data in the table shows that the proposed biometric quantum-based non-linear token key generation approach has better runtime performance on 2D/3D spinal images than traditional methods.

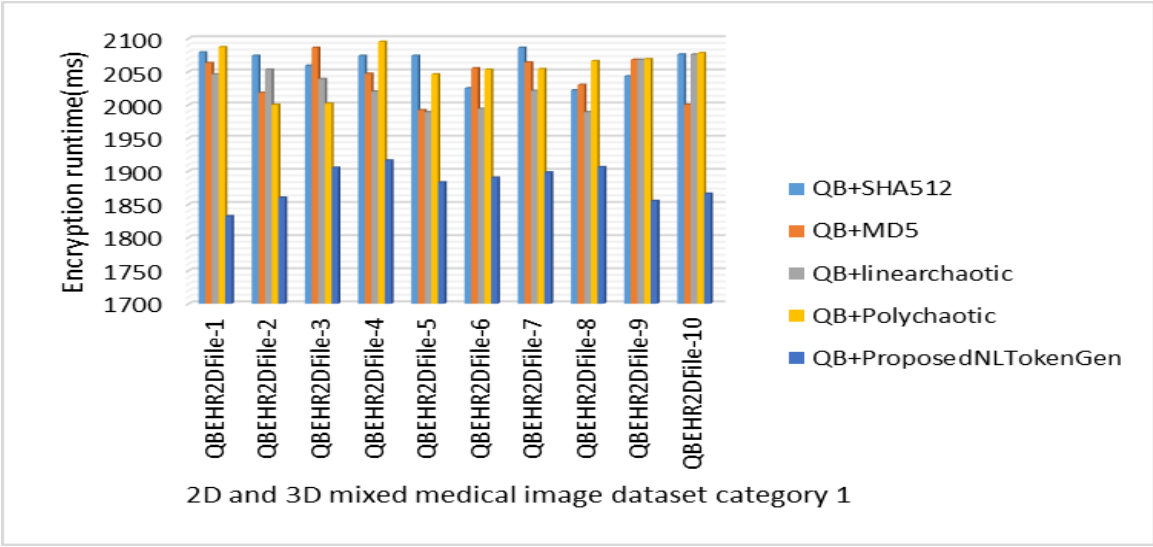

Figure 4: Comparative Analysis Of Quantum Biometric-Based Multi-User CP-ABE Scheme Encryption Runtime To The Conventional Approaches On 2D And 3D Category-1 Brain Images.

EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+Proposed NLTokenGen
QBEHR2DFile-1	2087	2000	2099	2014	1804
QBEHR2DFile-2	2087	2056	2030	2002	1819
QBEHR2DFile-3	2027	2019	2012	1994	1835
QBEHR2DFile-4	2063	2094	2027	2005	1896
QBEHR2DFile-5	2005	2079	2039	2052	1824
QBEHR2DFile-6	2044	2016	2085	2035	1815
QBEHR2DFile-7	2090	1993	2074	2010	1867
QBEHR2DFile-8	2048	2016	2063	1996	1842
QBEHR2DFile-9	2100	2056	2071	2032	1897
QBEHR2DFile-10	1998	2089	2052	2088	1904

Figure 4 compares the encryption runtime in milliseconds of a quantum biometric-based multi-user CP-ABE scheme for 2D/3D brain slices to conventional approaches. The data in the figure shows that the quantum biometric-based multi-user CP-ABE scheme has superior performance in terms of runtime on 2D/3D brain images compared to traditional methods.

Table 5: Comparative Analysis Of Quantum Biometric-Based Multi-User CP-ABE Scheme Encryption Runtime To The Conventional Approaches On 2D And 3D Category-2 Spinal And Category-3 Chest Images.

EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	2062	2049	2033	2028	1816
QBEHR2DFile-2	2002	2098	2041	2038	1894
QBEHR2DFile-3	2063	2035	2092	2001	1835
QBEHR2DFile-4	2041	2005	2098	2003	1816
QBEHR2DFile-5	2045	2010	2015	2091	1837
QBEHR2DFile-6	1991	2040	1999	1988	1838
QBEHR2DFile-7	2068	2009	2097	2043	1870
QBEHR2DFile-8	2083	2007	2011	2090	1897
QBEHR2DFile-9	2045	1991	2072	2021	1842
QBEHR2DFile-10	2020	2062	2070	2039	1865

Table 5 compares the encryption runtime in milliseconds of a quantum biometric-based multi-user CP-ABE scheme for 2D/3D brain slices to conventional approaches on 2D and 3D category-2 spinal and category-3 chest images. The data in the table show that the proposed quantum biometric-based multi-user CP-ABE scheme has superior performance in terms of runtime on 2D and 3D category-2 spinal and category-3 chest images compared to traditional methods.

Table 6: Comparative Analysis Of Quantum Biometric-Based Multi-User CP-ABE Scheme Encryption Runtime To The Conventional Approaches On Category-1 Brain , Category-2 Spinal And Category-3 Images

EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	4572	3479	4786	3166	2795
QBEHR2DFile-2	4563	3616	4526	3171	2878
QBEHR2DFile-3	4830	3638	4498	3326	2820
QBEHR2DFile-4	4866	3833	4619	3334	2818
QBEHR2DFile-5	4565	3766	4598	3190	2872
QBEHR2DFile-6	4741	3696	4855	3093	2854
QBEHR2DFile-7	4610	3780	4651	3052	2794
QBEHR2DFile-8	4867	3601	4487	3065	2836
QBEHR2DFile-9	4684	3484	4481	3116	2788
QBEHR2DFile-10	4805	3510	4707	3045	2864
EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	4805	3443	4667	3196	2841
QBEHR2DFile-2	4558	3484	4741	3113	2834
QBEHR2DFile-3	4832	3474	4693	3231	2792
QBEHR2DFile-4	4758	3752	4836	3139	2832
QBEHR2DFile-5	4548	3745	4793	3243	2891
QBEHR2DFile-6	4726	3815	4597	3322	2782
QBEHR2DFile-7	4627	3826	4551	3035	2837
QBEHR2DFile-8	4871	3855	4728	3195	2800
QBEHR2DFile-9	4487	3710	4586	3046	2850
QBEHR2DFile-10	4735	3491	4824	3069	2789
EHRTransactions	QB+SHA512	QB+MD5	QB+linearchaotic	QB+Polychaotic	QB+ProposedNLTokenGen
QBEHR2DFile-1	4663	3678	4592	3131	2834
QBEHR2DFile-2	4735	3680	4586	3049	2788
QBEHR2DFile-3	4470	3822	4827	3266	2832
QBEHR2DFile-4	4470	3623	4700	3304	2799
QBEHR2DFile-5	4538	3516	4869	3036	2848
QBEHR2DFile-6	4563	3473	4444	3040	2867
QBEHR2DFile-7	4499	3607	4547	3222	2832
QBEHR2DFile-8	4613	3816	4590	3151	2872
QBEHR2DFile-9	4448	3852	4723	3109	2832
QBEHR2DFile-10	4752	3517	4531	3341	2808

Table 6 compares the encryption runtime in milliseconds of a quantum biometric-based multi-user CP-ABE scheme for 2D/3D brain slices to conventional approaches on category-1 brain , category-2 spinal and category-3. The data in the table show that the proposed quantum biometric-based multi-user CP-ABE scheme has superior performance in terms of runtime on 2D and 3D category-1 brain , category-2 spinal and category-3 chest images compared to traditional methods.

5. CONCLUSION

In this paper, a quantum biometric-based multi-user ciphertext policy encryption and

decryption framework is proposed on the mixed 2D and 3D cloud medical records. Since, most of the conventional key generation models are difficult to create variable size key for the encryption and decryption process. Also, conventional attribute based encryption models are independent of token key for the user's authentication and security verification process. In this work, an advanced quantum biometric authentication based medical data encryption and decryption is proposed on the cloud medical records. Experimental results are evaluated on different medical records using token bit change and runtime computation. In the future work, a quantum key generation based cloud data security is proposed on the heterogeneous cloud medical records.

REFERENCES

[1] M. Ali, L. Tang Jung, A. Hassan Sodhro, A. Ali Laghari, S. Birahim Belhaouari, and Z. Gillani, "A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security," Alexandria Engineering Journal, vol. 64, pp. 749–760, Feb. 2023, doi: 10.1016/j.aej.2022.10.056.

[2] X. Wang, L. Bai, Q. Yang, L. Wang, and F. Jiang, "A dual privacy-preservation scheme for cloud-based eHealth systems," Journal of Information Security and Applications, vol. 47, pp. 132–138, Aug. 2019, doi: 10.1016/j.jisa.2019.04.010.

[3] D. Unal, A. Al-Ali, F. O. Catak, and M. Hammoudeh, "A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption," Future Generation Computer Systems, vol. 125, pp. 433–445, Dec. 2021, doi: 10.1016/j.future.2021.06.050.

[4] S. Shreya, K. Chatterjee, and A. Singh, "A smart secure healthcare monitoring system with Internet of Medical Things," Computers and Electrical Engineering, vol. 101, p. 107969, Jul. 2022, doi: 10.1016/j.compeleceng.2022.107969.

[5] M. Alloghani et al., "A systematic review on the status and progress of homomorphic encryption technologies," Journal of Information Security and Applications, vol. 48, p. 102362, Oct. 2019, doi: 10.1016/j.jisa.2019.102362.

[6] H. Hamidi, "An approach to develop the smart health using Internet of Things and authentication based on biometric technology," Future Generation Computer Systems, vol. 91, pp. 434–449, Feb. 2019, doi: 10.1016/j.future.2018.09.024.

[7] S. Krishnan, S. Lokesh, and M. Ramya Devi, "An efficient Elman neural network classifier with cloud supported internet of things structure for health monitoring system," Computer Networks, vol. 151, pp. 201–210, Mar. 2019, doi: 10.1016/j.comnet.2019.01.034.

[8] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," Computers & Security, vol. 97, p. 101966, Oct. 2020, doi: 10.1016/j.cose.2020.101966.

[9] A. H. Mohsin et al., "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," Computer Standards & Interfaces, vol. 66, p. 103343, Oct. 2019, doi: 10.1016/j.csi.2019.04.002.

[10] A. S. Alorfi, S. Yonbawi, S. Alahmari, A. A. Bozorboevich, M. Arumugam, and P. Q. Huy, "Biometric authentication integrated with wireless communication malicious activity detection in a cyber physical system-based Fintech banking," Optik, vol. 272, p. 170294, Feb. 2023, doi: 10.1016/j.ijleo.2022.170294.

[11] H. Wang, J. Liang, Y. Ding, S. Tang, and Y. Wang, "Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health," Computer Standards & Interfaces, vol. 84, p. 103696, Mar. 2023, doi: 10.1016/j.csi.2022.103696.

[12] C.-I. Fan and S.-Y. Huang, "Controllable privacy preserving search based on symmetric predicate encryption in cloud storage," Future Generation Computer Systems, vol. 29, no. 7, pp. 1716–1724, Sep. 2013, doi: 10.1016/j.future.2012.05.005.

[13] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," Future Generation Computer Systems, vol. 67, pp. 242–254, Feb. 2017, doi: 10.1016/j.future.2016.08.008.

[14] E. Zaghloul, T. Li, and J. Ren, "d-EMR: Secure and distributed Electronic Medical Record management," High-Confidence Computing, p. 100101, Dec. 2022, doi: 10.1016/j.hcc.2022.100101.

[15] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," Future Generation Computer Systems, vol. 85, pp. 76–87, Aug. 2018, doi: 10.1016/j.future.2018.02.040.
[16] M. Zhao E and Y. Geng, "Homomorphic Encryption Technology for Cloud Computing," Procedia Computer Science, vol. 154, pp. 73–83, Jan. 2019, doi: 10.1016/j.procs.2019.06.012.
[17] Z. Wu, S. Xuan, J. Xie, C. Lin, and C. Lu, "How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective," Computers in Biology and Medicine, vol. 147, p. 105726, Aug. 2022, doi: 10.1016/j.compbiomed.2022.105726.
[18] K. S. Patil, I. Mandal, and C. Rangaswamy, "Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption," Pervasive and Mobile Computing, vol. 82, p. 101552, Jun. 2022, doi: 10.1016/j.pmcj.2022.101552.
[19] Minahil, M. F. Ayub, K. Mahmood, S. Kumari, and A. K. Sangaiah, "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology," Digital Communications and Networks, vol. 7, no. 2, pp. 235–244, May 2021, doi: 10.1016/j.dcan.2020.06.003.
[20] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, D. Murillo-Escobar, and R. M. López-Gutiérrez, "Multibiosignal chaotic encryption scheme based on spread spectrum and global diffusion process for e-health," Biomedical Signal Processing and Control, vol. 78, p. 104001, Sep. 2022, doi: 10.1016/j.bspc.2022.104001.