WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Encryption Scheme For Data Sharing In Blockchain

AbiramiE[a],DhivyapriyaM[b], AbinayaR[c]

[a,b,c]SacredHeartArtsandScienceCollege,Perani,Villupuram605651,TamilNadu.

ABSTRACT:

In this project, we adopted a DNA security protocol using the AES (Advanced Encryption Standard) code set and blockchain system to verify the existing gift trading system. There are many situations where DNA testing is necessary. For example, the targets they are working on include DNA analysis, some crime analysis targets that are still needed, and disease analysis targets that are still needed. Therefore, a ll situations must be safe. We achieved this challenge by combining AES and blockchain technology. First of all, AES (Advanced Encryption Standard) is used to protect personal data, including DNA samples. AES is a recursive cipher, unlike the Feistel cipher. Merely as an "alternative" embodiment of the network "Blockchain is a system for recording information in a way that makes it difficult or impossible to alter, hack, or cheat the system. This is called decentralized database management. Individual genome statistics are cyber To protect or measure the privacy of their genomic statistics, the user of blockchain technology stores their genomic statistics. And by using the blockchain process in the hash value to perform these statistics and record the statistics. We already know that a blockchain is nothing more than endless blocks that can be woven together like a chain but also in a special cryptographic order. When it comes to secure data storage, little comes to mind other than blockchain. Since the blockchain itself is secure, distributed and transparent, we can see that the new birth of stable organizations is not hindered. The final message created is then stored securely in blockchain storage.

Keywords:Blockchain.

Introduction :

About the project:

Its purpose is so that hackers can target the weakest point when they need to access a system. The encryption system is no longer used. Users must ensure that the underlying software can perform the functions it is supposed to perform, properly protect user data, and modern technology is not good enough. DNA testing is used in all areas of law enforcement, including family law and criminal matters. Whether it's catching a killer or resolving a parent- child dispute, DNA can be used to match crimes to perpetrators. DNA evidence also plays an important role in court as evidence to prove a person's alibi. These include the purpose of the study, identification of the disease, and more. DNA matching is a very safe method. Missing persons, remains, unidentified persons, infected areas, criminal suspects, etc. can be used to define. As part of our job, we must take safety precautions during DNA testing. Additionally, there should be no gray areas or ambiguities in the storage and processing of data. It provides the backbone for storing, managing and analyzing data shared across multiple systems. Each web page in the ledger is a block in blockchain technology. Through a cryptographic hash, the block affects subsequent blocks or web pages. That is, when the block is completed, it creates a block or blockchain chain by creating different rules that link to the next web page or block. When the blockchain is transferred to a new blockchain transaction or a new block needs to be added to the blockchain, many nodes in the same blockchain application must perform algorithms to evaluate, validate and execute all blockchain data.

OBJECTIVE:

1. By encrypting the data, unauthorized users cannot read or understand it without the necessary decryption keys.
2. Encryption schemes enable participants to authenticate the origin of the data and verify the identity of the sender.
3. Encryption techniques help maintain control, allowing data owners to determine who can access their shared data and under what circumstances.
4. Encryption allows data owners to protect themselves and control others' access and use of their data.
5. Optimized encryption algorithms and methods are essential to maintain the performance of blockchain networks.
6. Standardizing cryptographic technologies and protocols helps improve compatibility and facilitates seamless integration of different blockchain systems.
7. The encryption process must be scalable to accommodate the size of the data and increase the number of participants participating in blockchain networks.
8. Once information is recorded on the blockchain, it cannot be changed or deleted, ensuring the integrity and integrity of the information.

SYSTEMANALYSIS

Existingsystem:

There are no security measures for the control of DNA samples in the current system. There are no security protections when writing sample content. It is used not only to collect DNA samples for testing but also for research. 9Therefore, inaccurate genomic data can harm research. In current systems, malicious users can easily access data. In this case, a malicious user can access and modify the data, which can cause a security vulnerability. In the current system, it takes a few days to get results. Since our system is not advanced technology, the accuracy of the results of existing systems is lower.

Disadvantages:

- The accuracy of the test is lower than the proposed method.
- Delivery of test results has been delayed.
- This will take a few days.
- There is no ID-based import process in the current system.

- For example, at the time of writing, no security measures had been taken to collect user details.
- There is no security mechanism for storing test data in the current system

Proposed system:

We ensured that each user received their ID in the request. Uploading and retrieving data based on ID is very easy for users. The system increases security by using encryption algorithms that never allow cyber attacks to occur. The encryption value is controlled by the monitor accessing the data. Users can receive notifications at a reasonable price determined by the management. In this system, the time from sample collection to results takes only a few days. Using blockchain technology, each page in the report forms a block. This block affects the next block or page using a cryptographic hash. That is, when the block is completed, it creates a unique security code that is associated with other pages or blocks, creating a blockchain or block chain.

Advantage:

- All processes are monitored with the help of management.
- It will help you avoid statistics. - Collection of samples and provision of information is mostly based on identity.
- This will help in getting the information cleanly.
- This document uses encryption algorithms to ensure that the individual can view important information.
- The most advanced technology is used to ensure the accuracy of the tests.
- This new technology helps make this process as much as possible.

SYSTEM METHODOLOGY

- User
- Admin
- Researcher
- Analyser
- Blockchain Storage

User:

In this model, when the user registers and wants to enter the user page, the test content, test status, application, payment and download menu will be transferred to the user's home page. After successful login, the user page will send the DNA sample data. When users submit DNA samples, it typically takes three to five days to receive results. Because there are many methods in DNA testing. After that the test conditions will be set and changed by the administrator. This is useful because its users can easily determine whether the results are intended or not. When the results are ready, the user will request areport from the administrator. When the request is sent to the administrator, the administrator will respond to the user.

Admin:

In this mode, when the admin wants to enter the admin page, it will switch to the admin homepage, which shows View Team Content, View Team Comments, Update Request and Payment Show on the admin homepage. The administrator will check the registration information of the research team. When the registration information is correct, only the administrator will approve the next run, otherwise further work will be allowed. Authorities will send DNA samples to the investigation team.

Reseacher:

In this mode, if the research team wants to register and log in with its content, it will return to the research team homepage showing the registration, viewing status, decryption, process and submission menu items. The initial research team wanted to record their content on the registration page. Then wait for the administrator's approval, when the registration is completed, the administrator will check the registration information and if it is correct, the administrator will approve the research team. Once approved, encrypted sample content is made available. Finally install the instructions step by step.

Analyser :

In this change, if the analyst group wants to register and log in with its content, it will go to the analyst group homepage, which will display the registration form, view the status layer, write content, and publish reports. The first group of analysts want to save their content on the registration page. Then wait for the administrator's approval; The administrator will check the registration information after the registration is completed. If true, the manager will agree with the audit team. Once approved, get step-by-step instructions. Comparing the ports will take a few minutes. Once the campaign is complete it will take a few minutes for the report to download. Previously published documents are stored on the blockchain in blockchain format.

Blockchain Storage:

In this module the blockchain storage wants to register and log in with their details, it will redirect to the blockchain storage home page which has research team registration details, analyzing team registration details, sending the report, stored data, and backup data menus displayed on the blockchain storage page. The first research team and analyzing team registration details are stored, both are store in separately. Then checking the report request by the user or admin. If any request is there, then blockchain storage will send report data to the admin. Then the stored report data are in block chain method in hash values using the private key. There is a backup also provided by the storage.

CONCLUSION:

Our proposed version uses a blockchain method to store data through blockchain technology, where each page of the report is written as a block. Many different situations require the DNA testing process due to many different factors. Crime analysis, research purposes, disease analysis etc. can be used for other purposes. In general, security is required in these situations. Since our profession requires safety during DNA testing, we work hard for this. This block affects the next block or page using a cryptographic hash. In other words, when a block is completed it creates a unique security code that is associated with the next page or block, creating a blockchain or chain of blocks. Collecting DNA samples from users and collecting users' personal information is highly secure due to the AES encryption process. Because when hackers want to enter a system, they focus on weak points. Whether it is a 128-bit key or a 256-bit key, this is generally not the encryption of the system. Users must ensure that the software they are considering performs the functions they need, properly protects user data, and that the entire process is error-free. It will be developed and used in the future to adapt to the needs of the situation.

REFERENCE:

1. **https://www.hindawi.com/journals/wcmc/2022/1040662/**
2. https://onlinelibrary.wiley.com/doi/10.1002/cpe.7896
3. **https://ieeexplore.ieee.org/document/8751336**
4. https://www.computer.org/csdl/journal/bd/2023/06/10175626/1OAJfwfkxZC