Fair Characteristic-Primarily Based Totally Encryption Scheme For Data Sharing In Blockchain

D.Hariharan[1], P.Haripradhap[2], M.Vignesh[3], M.Monishkumar[4], Mrs. K. Shanthi Ponraj[5]
[1, 2, 3, 4] Dept of Information Technology
[5]AP, Dept Of IT
[1, 2, 3, 4, 5]Sri Muthukumaran Institute Of Technology

Abstract- *In this project we have proposed secure DNA checking out the procedure for the already gift venture using the set of rules AES and blockchain procedure. There are lot of situation that would be needed for DNA checking. The main purpose of this is to produce a secure way in this field. In the mixture of AES and blockchain techniques, we've put into force this challenge. Firstly AES used the securely cope with the person's private info and additionally the gathered DNA pattern info. AES is an iterative as opposed to a Feistel cipher. It is primarily based totally on the "substitution- permutation network Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. That while is called decentralized database management. A person uploads his private genome statistics to a web genomics studies center. To guard or test the confidentiality of his genome statistics, the person store his genome statistics with an blockchain techniques. And processing those statistics and saving the statistics through the use of the blockchain approach in hash values. We recognize that blockchain is not anything but a countless inundation of blocks that can be knit collectively like a chain, and that too in a particular order of cryptography. When it involves securely storing data, there may be hardly ever something that pops up in our idea terrains aside from blockchains.*

Keywords- Attribute-based proxy re-encryption, block chain, Data sharing, Cloud computing, Verifiability, Fairness.

I. INTRODUCTION

The mission is that when hackers need to gain access to a system, they may target the weakest link. Users must make certain the software program below attention does what they need it to do, that it protects consumer information in the manner it is anticipated to, and that the general technique has no susceptible points. DNA testing is being used in all fields of law enforcement, including family law and criminal cases. DNA evidence also plays a major role in the all areas, where it can be presented as proof that someone was at the scene of the crime when they weren't. It can be used to identify missing persons and human remains, individuals who have obtained false identities, the source of outbreaks of contagious diseases, and criminal suspects. We must achieve security during the DNA checking procedure as part of our project. Furthermore, there must be no grey areas or uncertainty regarding information storage and handling. It provides a backbone to store, manage and analyze data that is shared across many systems. Every web page in a news ledger is a block in Blockchain technology. Through cryptographic hashing, this block influences the following block or web page. In other words, when a block is completed, it generates a one-of-a-kind consistent code that is linked to the next web page or block, thus growing a chain of blocks or a blockchain. When a blockchain is delivered to a new blockchain transaction or a new block is to be added to the blockchain, several nodes in the same blockchain implementation are required to execute algorithms to evaluate, confirm, and process the blockchain's record.

II. LITERATURE SURVEY

[1] SECURITY CHALLENGES FOR THE PUBLIC CLOUD

- K. Ren, C. Wang, and Q. Wang

Abstract

This paper surveys about the various cryptographic techniques with their key sizes, time required for key/signature generation and verification constraints. The survey discusses the architecture for secure data transmissions among the devices, challenges raised during the transmission and attacks. This paper presents the brief review of major cryptographic techniques such as Rivest, Shamir Adleman (RSA), Diffie Hellman and the Elliptic Curve Cryptography (ECC) associated key sizes. This paper investigates the general impact of digital signature generation techniques on cloud security with the advantages and disadvantages. The results and discussion section existing in this paper investigate the time consumption for key/signature generation and verification with the key size variations effectively. The initialization of random prime numbers and the key computation based on the points on the elliptic curve assures the high-security compared to the existing schemes with the

minimum time consumption and sizes in cloud-based applications.

[2] ATTRIBUTE-BASED ENCRYPTION WITH VERIFIABLE OUTSOURCED DECRYPTION
-J. Lai, R. H. Deng, C. Guan, and J. Weng
Abstract:

With Hidden Credentials Alice can send policy-encrypted data to Bob in such a way that he can decrypt the data only with the right combination of credentials. Alice gains no knowledge of Bob's credentials in the process, and hence the name "Hidden Credentials." Research on Hidden Credential systems has focused on messages sent to single recipients, where the sender needs to know the recipient's pseudonym beforehand, and on Hidden Policies, where Bob learns as little information as possible about Alice's policy for decrypting the message. Current schemes provide weak policy privacy with non-interactive schemes, the recipient can learn parts of the policy, and with interactive schemes based on secure multiparty computation, a user can try different sets of credentials as input to gain knowledge of the policy after repeated decryption attempts. Furthermore, existing schemes do not support policies with negations efficiently. For example, a policy stating "Bob is not a student" is hard to enforce since Bob can simply withhold, or not use, his student credential.

III. METHODOLOGY

First, we present a formal definition of VF-ABPRE which considers the verifiability and fairness of attribute-based encrypted data sharing in cloud computing.

Then, we construct a concrete VF-ABPRE scheme and prove its confidentiality, verifiability and fairness.

Finally, we conduct an implementation to evaluate the performance of our proposed scheme to demonstrate its practicality and efficiency.

PROPOSED SYSTEM

In the proposed system, we have implemented that each user gets their ID. Based on the id, the upload and retrieval of the data are very convenient for the user. This system has the enhancement of security, by implementing the encryption algorithm which may never allow the cyber-attacks to happen. The encrypted values have been controlled with an administrative view, which makes the authorized to access the file. The user can get the report at a reasonable price, which was fixed by the administration. In this system, results can take only few days from the collection of samples. AES is used to securely gather and process the person's private info and additionally their DNA pattern. With Blockchain technology, each page in a ledger of reports forms a block. This block has an impact on the next block or page through cryptographic hashing.

ADVANTAGES

- The overall process is monitored with the aid of using the administration. It will assist to save you from statistics leakage.
- The collection of samples and retrieval of the report is primarily based totally on the id.
- The encrypted algorithm is used in this data which makes privacy to see the important data.
- Advanced techniques used to achieve good accuracy in test reports.
- This new techniques are help to quick these processes as much as possible.

IV. MODULES

1.USER MODULE:

In this module the user wants to register and log in to the user page. After successful login, the user page then uploads the DNA sample details. Then that test status will be updated, which was updated by the admin. Once results are ready then the user will request the admin for the report. Then the admin will request the blockchain storage and get the report data and set the payment amount to that report data. Once the payment is completed, user will get the key from the admin and retrieve the report data and download it.

2.ADMIN MODULE:

In this module the admin wants to log in to the admin page, which has some components. Then admin will check the research team registration details. Once the registration details are correct then only the admin will approve to further process. After that admin will send the DNA sample details to the research team in encrypted format. Then admin will check the analyzing team registration details. Then admin will monitor all processes and continuously update the test status. Then the admin will get request from the user and respond with the payment method.

3.RESEARCHING MODULE:

In this module the research team wants to register and log in with their details. The first research team wants to

register their details on the registration page and wait for the approval from the admin. Once they got the approval, they will get sample DNA in encrypted form. They generate decryption key for encryption. There are two processes are done by the research team, one is the extraction process the DNA molecules are extracted from the given sample. And extracted DNA molecules are in low quantity because of sample quantity is low. So that the multiplying process is carried out and the sequencing of the DNA molecules. Finally, upload the sequencing details.

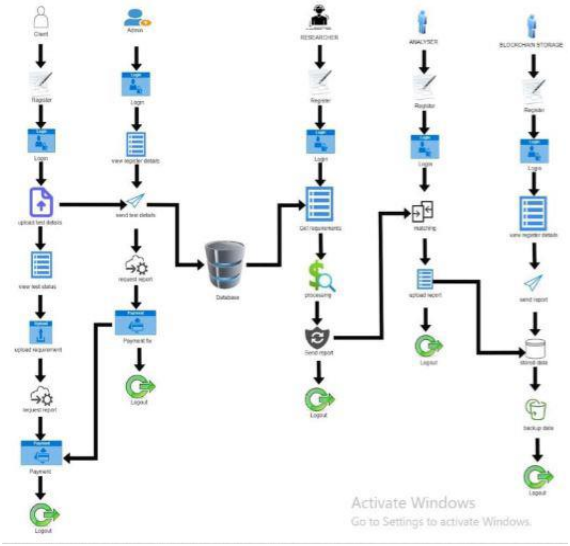
4.ANALYSING MODULE:

In this module the analyzing team wants to register and log in with their details. The first analyzing team wants to register their details on the registration page. Then they will wait for the approval from the admin and after the approval they will get the sequencing details. Then matching the sequencing details will take a few seconds. After that matching successfully then downloading the report will take a few seconds. Then upload the previously generated report to the blockchain storage in the block chain method.

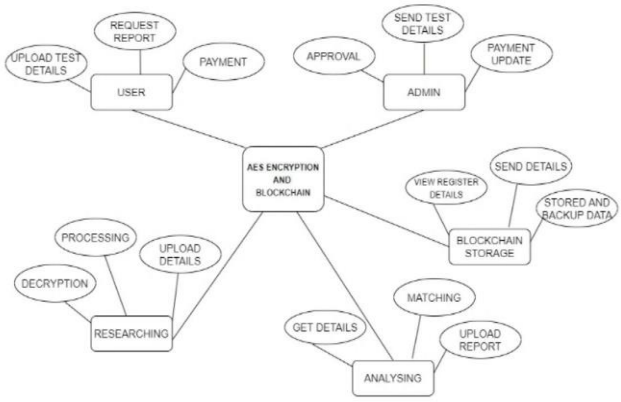
5. BLOCKCHAIN STORAGE MODULE:

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.

ARCHITECTURE DIAGRAM



ER DIAGRAM



V. CONCLUSION

Our proposed version has applied the blockchain method for storing the report With Blockchain technology, each page in a ledger of reports forms a block. Many different situations are requiring DNA testing procedures to be carried out as a result of different factors. It can be used for analysis of crime, for research purposes, for the analysis of disease, etc. In most cases, security is necessary in those situations. Our project calls for ensuring security during the DNA testing process, and as a result, we are trying to do so. This block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks or a blockchain. And the collection of DNA samples from users and the collection of user personal details are highly secure because of using the AES encryption process. Because when hackers want to access a system, they will aim for the weakest point. This is typically not the encryption of a system, regardless of whether it's a 128-bit key or a 256-bit key. Users should make sure the

software under consideration does what they want it to do, that it protects user data in the way it's expected to and that the overall process has no weak points. In the future, it has been enhanced and applied with experimentation for an effectively needed situations.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89– 98.

[3] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in International Conference on Information Security Practice and Experience. Springer, 2009, pp. 13–23.

[4] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in International Workshop on Public Key Cryptography. Springer, 2013, pp. 162–179.

[5] N. Attrapadung, B. Libert, and E. De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in International Workshop on Public Key Cryptography. Springer, 2011, pp. 90–108.

[6] J. Herranz, F. Laguillaumie, and C. Rafols, ` "Constant size ciphertexts in threshold attribute-based encryption," in International Workshop on Public Key Cryptography. Springer, 2010, pp. 19–34.

[7] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu, and C. Rafols, ` "Attribute-based encryption schemes with constant-size ciphertexts," Theoretical computer science, vol. 422, pp. 15–38, 2012.

[8] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in International Conference on Provable Security. Springer, 2011, pp. 84–101.

[9] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in Annual Cryptology Conference. Springer, 2012, pp. 180–198.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Lecture Notes in Computer Science, vol. 2008, pp. 321–334, 2011.