IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104273 |

Blockchain Based Identity Verification System

Prof. N.B Vairagde[*1] Avinash Waghmare [*2], Nilesh Deshmukh[*3], Prajkta Thool[*4], Mayur Darunde[*5], Sunil Wete[*6]

[*1]Professor, Department of Computer science & Engineering SSPACE, Wardha Maharashtra, India

[*2,3,4,5] Student, Department of computer science &Engineering SSPACE, Wardha, Maharashtra, India

ABSTRACT: It is based on Cyber security dataset Cloud services have increased the number of data owners it has been store their encrypted data in the cloud, while an equal or greater number of data users based in data retrieval.It is based on Block chain Hybrid ECC and AES Algorithm using the Encrypted and Decrypted the dataset. Encrypted File will be Stored in Cloud Server and User based on Keyword Searching for Algorithm. User based Enter the keyword that also Encrypted Query After that Searching Encrypted Cloud Server Finally Retrieval the Related File on Query based. User based enter the Particular key user decrypts File the better performance better performance in terms of recall, ranking privacy, precision, searching time

KEYWORDS: Blockchain, Self- sovereign Identity, authentication mechanism, Identify proofing, claim verification.

I. INTRODUCTION

- Identity theft is the unauthorized acquisition of another person's confidential information in order to misuse it.
- In any registration process we have to bring physical document that causes unauthorized access of users personal document.
- A BLOCKCHAIN TECHNOLOGY can solve this problem.
- In this, a system called Blockchain-based personal Identity security System is proposed whereby it is a system which stores an individual's personal records on the blockchain.
- This system uses the security features of blockchain to allow everyone to know who has access to their data

II. METHODOLOGY

In this research, our motivation is to develop a concept that maximizes the transparency as well as the control over personal data for users. My Data has proposed a human-centric approach that empowers the user by placing him in the center of his data ecosystem.

The main focus here is not owning the data (i.e. storing the data on the user's own server), but to control the data flow from data to service provider by controlling the associated consents from the user to the respective service. While the approach of My Data, requires a significant shift in the ecosystem and that service providers agree on this way of handling data, we sought to develop an approach that can enable a fair balance in the ecosystem without support from the service provider, but only through technology and legislative means.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104273 |

III. MODELING AND ANALYSIS

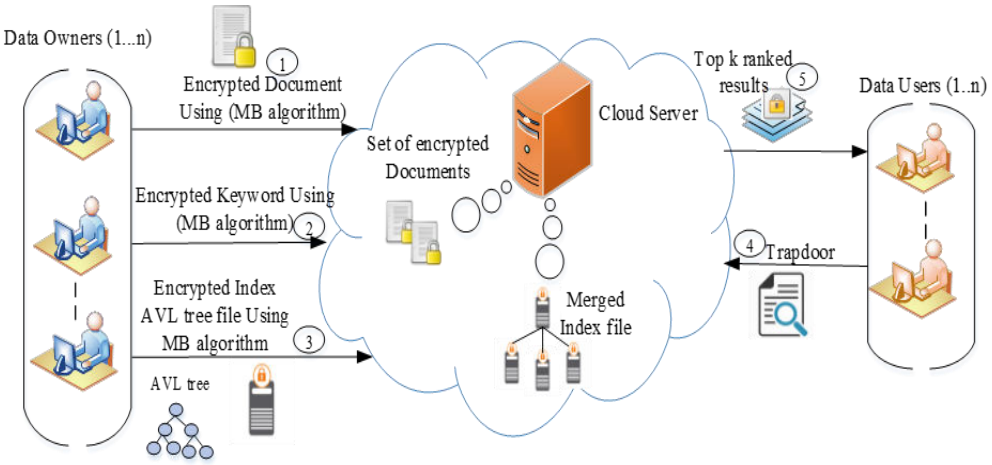

Figure 1: Architecture

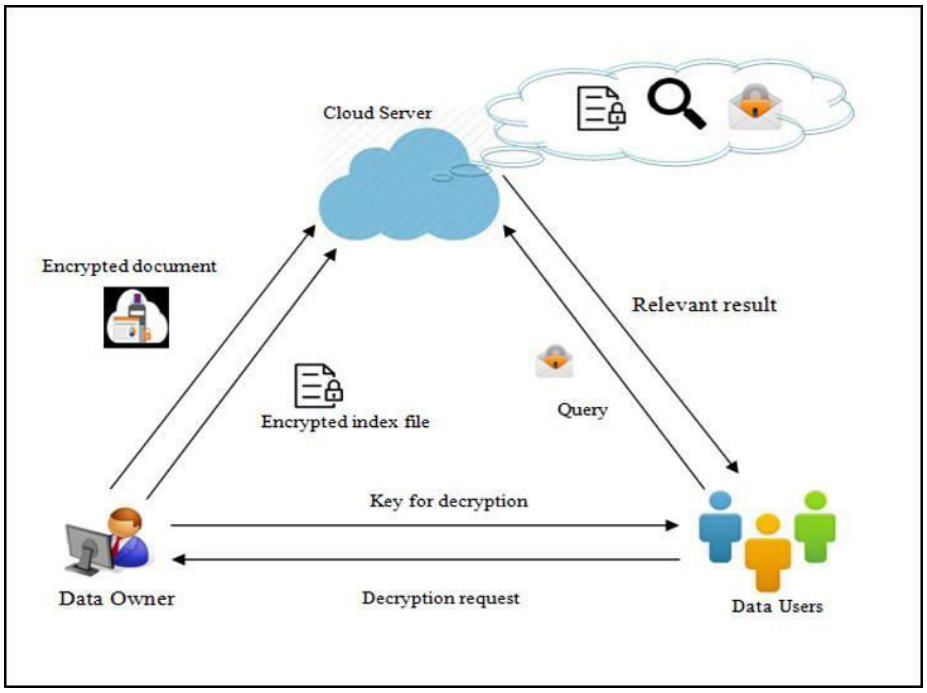

Figure 2: Blockchain Based Identity Verification System

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104273 |

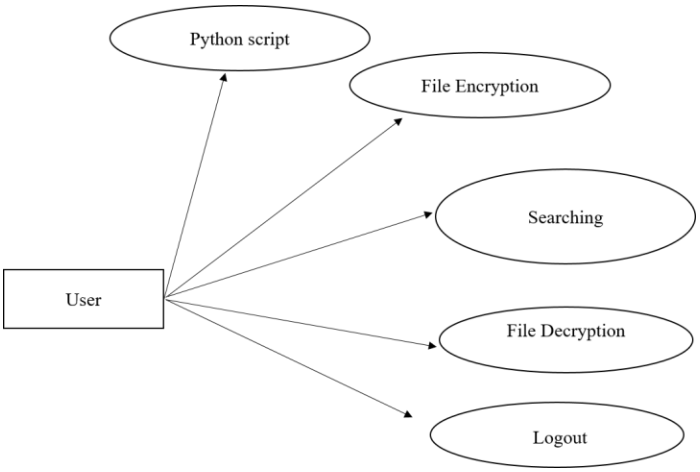

Figure3: Use Case Diagram

- A user wants to access a service, which the provider requests information for
- The user authenticates himself to the personal data storage through his private key
- A consent transaction is created on the blockchain with a shared identity of the service provider and the user. This gives the provider access to that data point as well as the identity blockchain
- The service provider can read run the information through the stored hash and verify the information the user has successfully identified himself and the provider has only the information needed.

IV. DATA SELECTION

- Cyber security is the use of technologies, processes, and controls to defend against cyber-attacks on systems, networks, programs, devices, and data.
- Its goal is to reduce the risk of cyber-attacks and to protect against unauthorized use of systems, networks, and technologies.
- Cyber security Protocols Reference and Keywords
- In this step, we have to load the data with the help of panda's packages

V. DATA PREPROCESSING

- Data pre-processing is the process of removing the unwanted data from the dataset.
- Pre-processing data transformation operations are used to transform the dataset into a structure suitable for machine learning.
- Missing data removal: In this process, the null values such as missing values and Nan values are replaced by
- as variables with a finite set of label Encoding Categorical data: That categorical data is defined values.

VI. HYBRID ECC AND AES ALGORITHM

- ECC Elliptic Curve Cryptograph Algorithm based on Public and Private Key
- ECC and AES based on Encrypted data
- The quick explanation is that keys using Elliptic Curve Cryptography (ECC) are asymmetric (public and private), whereas AES-256 uses a symmetric cypher (key)
- ECC and AES based on it Public and Private key
- Hybrid AES and ECC based on **128 bit key** Generated For Encrypted data Wise

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104273 |

VII. KEY GENERATION

- Hybrid AES and ECC based on 128 bit key Generated For Encrypted data Wise
- A encryption system is designed by combining the characteristics of the AES and ECC
- Which Can solve Security Problem itself
- Efficiently realize the information, data encryption, signature, and identity verification

VIII. CLOUD ME

- Encrypted File Will be Stored in data for Security purpose
- A cloud computing model in which data is stored on the Internet via a cloud computing provider who manages and operates data storage as a service
- Cloud Server will be used on Cloud me Software

IX. RESULTS AND DISCUSSION

Regarding the testing which is part of the transition phase, there were two types of testing done: system and acceptance testing. The summary of test cases is in Table 2, whereby there were a total of 18 cases for each of the functionalities in the web application as well as the Android application. The functionalities are as follows: authority, requester and user registration, authority and user log in, upload user details, and request user details.

X. CONCLUSION

Hybrid ECC and AES Algorithm using the Encrypted and Decrypted the dataset
Encrypted File will be Stored in Cloud Server and User based on Semantic Searching method Algorithm. User based keyword Entering is done to retrieve the corresponding data file from the cloud storage.
Finally Retrieve the Related File based on Query.
This will easily Find out **Cyber security Problem** like, the fault file will be detected

REFERENCES

1. Pascual, A., Marchini, K., & Miller, S. (2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Retrieved from https://www.javelinstrategy.com/coverage-area/2018-identityfraudfraud-enters-new-era-complexity
2. O. N. Guy Zyskind and A. S. Pentland. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data
3. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7013169
4. https://academicjournals.org/journal/JLCR/article-full-textpdf/8599A6F7684
5. https://www.researchgate.net/publication/222808883_Biometricbased_personal_identityauthentication_system_and_security_analysis
6. Yasin, A., & Liu, L. (2016). An Online Identity and Smart Contract Management System. In 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Atlanta, GA: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7552202

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details