LEVERAGING THE SELECTED BLOCKCHAIN TOOLS AND TECHNIQUES IN ENHANCING THE EFFICACY OF MOBILE FINGER PRINT VERIFICATION

Shubham Bhardwaj

National Institute of Technology, Hamirpur, Himachal Pradesh

ABSTRACT:

Biometric identification has gained popularity in recent years. Due to the rising usage of cloud computing, the management of databases is encouraged to store huge amounts of identification and biometric data on the cloud server. They will save money on storage and computation costs because of this, but users' privacy may be compromised. This paper proposes a private and efficient outsourcing method for biometric identification. Additionally, after the encryption of biometric data, it is distributed to the blockchain. The database owner encrypts the search query while sending the biometric identification data to the Cloud. The encrypted database contains the results of the Block Chain's identification procedures for the owner. Even if hackers can forge identification requests and work with the Cloud, a comprehensive security analysis reveals that the proposed plan is secure.

INTRODUCTION

With the development of Innovation, effectiveness and protection safeguarding is the significant issue, so here, utilizing Biometric distinguishing proof for individual confirmation. The comprehensive security analysis demonstrates that the proposed plan can protect the necessary privacy. Our proposed system targets and protects against the suggested systems attack and secures it under the biometric identification redistribution model. Analysis of execution shows that the suggested work has less training and computational identification costs than the current detection schemes. An effective biometric identification system that protects privacy can stop user collusion attacks. Attackers can view only the cloud-stored encrypted data. The well-known cypher text-only model has been implemented to avoid this. Security is enhanced through the enhancement of blockchain features and the integration of blockchain technologies with fingerprint verification. Data, a hash, a random number, a previous block, a timestamp, and transactions are all contained in the blocks. Because each block is intertwined, it is difficult to encrypt and impossible to connect the data in the blockchain. The information is stored in a cloud server to prevent unauthorised access.

OVERALL ARCHITECTURE

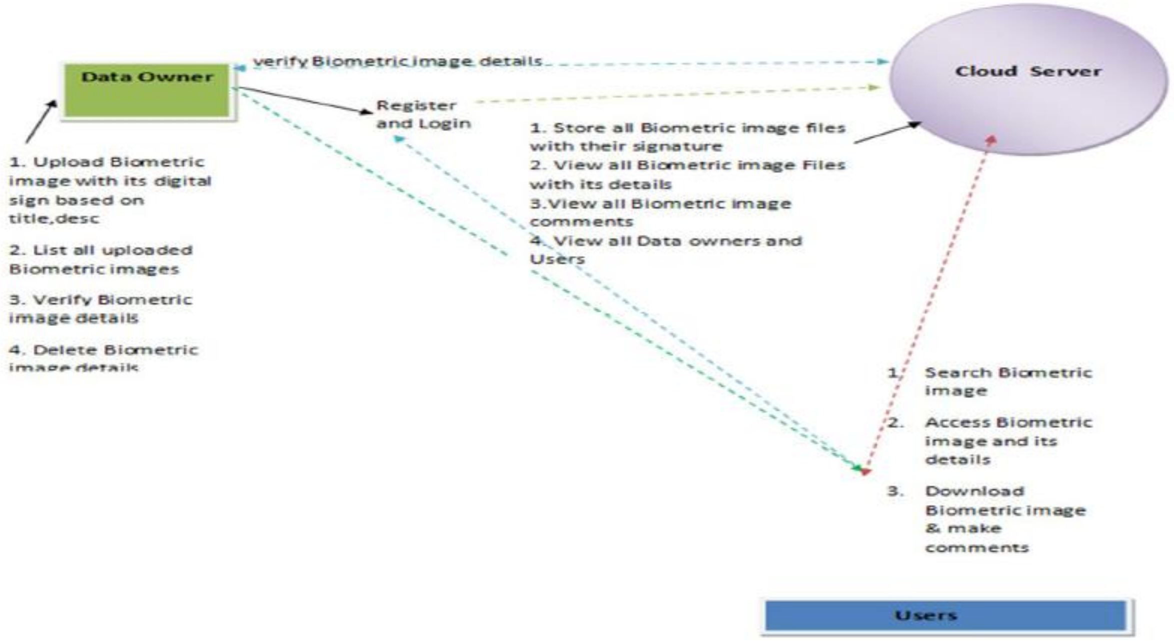
Data Owner
verify Biometric image details
Cloud Server
Register and Login
1. Store all Biometric image files with their signature
2. View all Biometric image Files with its details
3.View all Biometric image comments
4. View all Data owners and Users
1. Upload Biometric image with its digital sign based on title,desc
2. List all uploaded Biometric images
3. Verify Biometric image details
4. Delete Biometric image details
1. Search Biometric image
2. Access Biometric image and its details
3. Download Biometric image & make comments
Users

Figure 1: Architecture Diagram of Proposed Work

Figure 1 shows the Engineering Chart of the proposed framework where every one of the points of interaction between the Client, Information Owner, data are shown and made sense of below.

A cloud is managed by a company that offers data storage services. 1) Who owns the data: The information owner transfers their Biometric pictures and items information to the Cloud server in this module. As depicted in Figure 2, the system comprises three entities: users, the database owner, and the Cloud. The owner of data chooses the digital signature, stores it securely in the Cloud, uploads biometric images with their digitally signed based on identification and characterisation, lists all uploaded biometric images, verifies biometric image details, and removes biometric image details. And carries out the following actions: stores all biometric image files along with their signature; looks at all biometric image files and their details; looks at all biometric image comments; looks at all data owners and users, and looks at all attackers. Permission is given to the cloud users to access and modify the stored biometric images and user data. They also have a right to store a large amount of data on the cloud. If permission is given to the end client, they can search and access the biometric data only by following the below-given steps: Search the biometric image; Access the biometric data and its image; Download the biometric image and Make comments. The database owner has access to a significant portion of biometric data, such as iris, voice, and fingerprint patterns, which are stored in the Cloud in encrypted form. When a user wants to self-determine, the user sends a search query request to the database owner. The database owner generates the ciphertext for the biometric feature upon receiving the request and then sends the ciphertext for identification to the cloud server. The cloud server decides the best counterpart for the scrambled inquiry and returns the corresponding file to the data set proprietor. Eventually, the database admin returns the search query results to the user after computing the similarity between the searched query and the biometric data based on the index. Hashing public data makes use of the SHA256 algorithm.

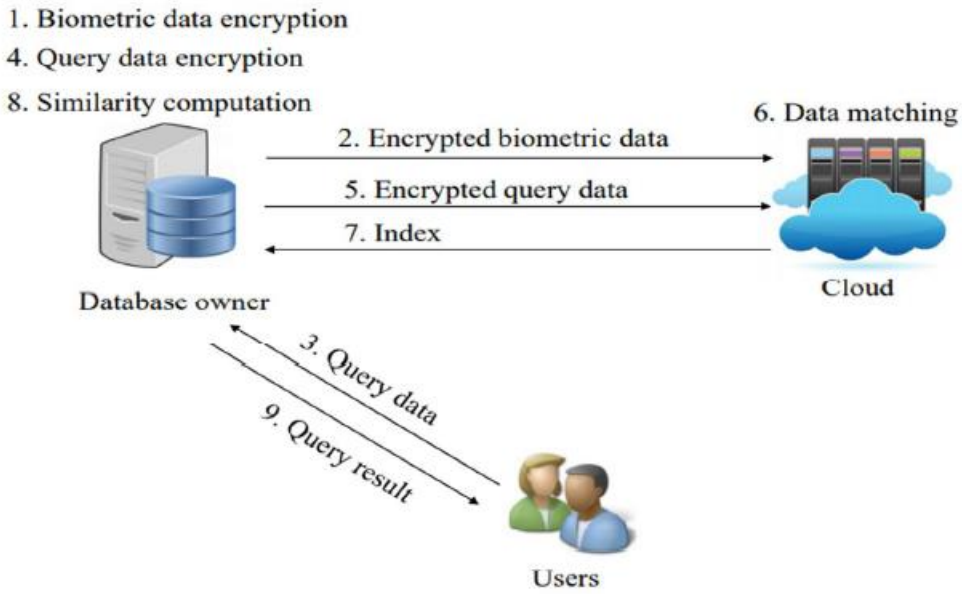

Figure 2: Diagram showing Workflow

IMPLEMENTATION

The project's development is broken up into several stages, making it simple for programmers to create software. The realization stage is one of the most crucial phases. The designer creates the front view, and the programmer is involved in coding. Which should utilize architecture and programming language? Will check all requirements to see if they are met at the end of this phase. Application development is done with the Eclipse Environment (IDE). As a programming language, Java is utilized.

1) Who owns the data: The owner of database stores a biometric data which is of significant amount in this module, including fingerprints, images, facial patterns, and so on. which is encoded and communicated to the Cloud for capacity. When a user wishes to self-identify, a query request is sent to the owner of the database. The database owner creates a ciphertext for the biometric trait upon receiving the request and then sends the ciphertext to the Cloud for identification. The data owner sends their biometric images and associated data to the cloud server. For security reasons, the data owner assigns the digital sign, stores it in the Cloud, and then does the following: Based on the title and description, upload a biometric image and digital sign; Listing of all uploaded biometric images; Verify specifics of biometric images; Remove details from biometric images.

2) The Cloud Server: The Cloud specialist co-op deals with a Cloud to give information capacity administration. Here, digital data is stored in a model of computer data storage known

as cloud storage. When the Cloud gets the code text from the proprietor, it first mists the server, sorts out the best counterpart for the encoded inquiry and returns the connected list to the information base proprietor. And carries out the following actions: View all biometric image comments, all Data owners and users, and all attackers. Stores all biometric pattern files with their sign. View all biometric image files with user details.

3) User: The Cloud Client who needs to get a lot of information from the proprietor is put away in Cloud Servers and has the authorization to get to and control put away Biometric picture and their information. Before a query request is sent to the owner, the users must first obtain permission from the server. It is forwarded to the Cloud. After receiving authorization, the customer will search the data, access the biometric image data, and carry out the following actions: Search the biometric image; Access the biometric image and its details; Download the biometric image; and Comment on the biometric image.

CONCLUSION

Utilizing the inherent structures of biometric data and identification operations, we first present a single-server, privacy-preserving biometric identification method.To address the issues for both productivity and security, we've made another encryption and cloud confirmation certificate. The comprehensive analysis reveals that it can defeat potential threats. Performance reviews also demonstrated that the proposed framework meets the requirement for efficacy well. In addition, they outsource this time-consuming scanning while maintaining database and computation privacy.

REFERENCES

[1] On Implementing Deniable Storage Encryption for Mobile Devices Adam Skillen and Mohammad Mannan Concordia Institute for Information Systems Engineering Concordia University, Montreal, Canada {a skil, mmannan}@ciise.concordia.ca .Related from https://users.encs.concordia.ca/~mmannan/publications/mobiflage-ndss2013.pdf

[2] Higgins S (2016) Hours after launch, OpenBazaar sees first drug listings. CoinDesk. Retrieved from http://www.coindesk.com/drugs-contraband-openbazaar/. Accessed 1 June 2018 Data leakage mitigation for discretionary access control in collaboration clouds January 2011

[3] How to Build a Trusted Database System on Untrusted Storage.January 2000,Author Maheshwari u, Vingralek R ,Shapiro Retrived from https://www.researchgate.net/publication/220851794_How_to_Build_a_Trusted_Database_System_on_Untrusted_Storage

[4] Attribute-based fine-grained access control with efficient revocation in cloud storage systems. Authors: Kan Yang, XiaohuaJia, KuiRen Year: 2013 Retrived from https://ece.uwaterloo.ca/~kan.yang/paper/C10-AsiaCCS.pdf

[5] Secured Electronic Voting System Using the Concepts of Blockchain Authors: Sudharsan B ; Rishi Tharun V ; Nidhish Krishna M P ; Boopathi Raj J ; Surya Arvindh M ; Dr. M. Alagappan Year:Oct. 2019 . Retrived from https://ieeexplore.ieee.org/document/8936310

[6] Fully secure key-policy attribute-based encryption with constant- size ciphertexts and fast decryption. Authors: Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al Year: Jun. 2014 Retrived from https://www.researchgate.net/publication/266656648_Fully_secure_key-policy_attribute-based_encryption_with_constantsize_ciphertexts_and_fast_decryption

[7] SDSM: a secure data service mechanism in mobile cloud computing. Authors: Jia W, Zhu H, Cao Z, et al Year: 2011 Retrived from https://www.researchgate.net/publication/224243124_SDSM_A_secure_data_service_mechanism_in_mobile_cloud_computing

[8] Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. Authors: Benjamin Livshits, Jaeyeon Jung Year: Aug. 2013.Retrived from https://www.researchgate.net/publication/261849235_Automatic_mediation_of_privacy-sensitive_resource_access_in_smartphone_applications