IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

COGNIZENT BIOMETRIC RECOGNITION WITH EFFICIENCY AND PRIVACY PROTECTION

[1]Dr. N.V. RAMANA REDDY, [2]YANNAM SUMANTH REDDY,
[1]Associate Professor, [2]UG STUDENT
[1,2]DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS
[1,2] AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY
Gunthapally(V), Abdullapurmet(M), R.R Dist

Abstract: The project " Cognisant Biometric Recognition with Efficiency and Privacy Protection " aims at providing a secure and efficient biometric authentication system using cloud computing and encryption techniques. The system is designed to secure sensitive biometric data such as fingerprints, facial features, iris scans, and other personal identification data while allowing for quick and accurate identification of users. However, privacy leakage and unauthorised access of the biometric data are the major challenges in the conventional biometric system. To overcome these issues, the proposed system encrypts the biometric information before storing that in the cloud, so that the information is confidential and the communication between users, database owners and cloud servers is secure.The system consists of three main modules: Database Owner, User and Cloud Server. The biometric data is uploaded to the cloud by the database owner and encrypted. The user sends a biometric query request for identification and the cloud server computes the encrypted query to retrieve the best matching biometric record, without exposing sensitive contents. The cloud securely returns the result to the database owner and user. Such approach improves the recognition efficiency and privacy protection simultaneously.The project is developed using Java technology, JSP, JDBC, MySQL and networking concepts. Platform independence, security, robustness and object-oriented features of Java make it suitable for developing secure biometric applications. The system also employs encryption mechanisms, secure data transmission, and database connectivity to ensure reliable storage and processing of biometric information.In conclusion, the proposed biometric recognition system improves the accuracy of authentication, minimises security risks, and maintains user privacy in cloud-based environments. The project shows how to combine secure biometric systems with cloud computing technologies to achieve reliable, scalable and privacy preserving user identification.

Keywords— Biometric Recognition, Cloud Computing, Privacy Protection, Data Encryption, Secure Authentication.

I. INTRODUCTION

Now biometric recognition systems form an important part of modern security and authentication applications. They can accurately identify people using biological characteristics that are unique to each individual such as fingerprints, facial patterns, iris scans and voice recognition. These systems are used extensively in banking, healthcare, military services, smart devices, access control systems, and cloud-based applications as they provide better security than the traditional password-based authentication methods. But the rapid expansion of cloud computing and online storage of data has brought up serious concerns about the privacy and security of biometric data.

Traditional biometric systems typically store sensitive user data in centralised databases which are susceptible to unauthorised access, data leakage, identity theft, and cyberattacks. Because biometric data is unique and permanent for each individual, any compromise of this information can lead to serious privacy risks. Thus, it is a great research challenge in the field of cybersecurity and cloud computing to protect biometric templates, while maintaining an efficient recognition performance.

The project "Cognizant Biometric Recognition with Efficiency and Privacy Protection" aims to develop a secure and efficient biometric authentication framework that guarantees user privacy and enables accurate identification. The proposed system uses biometric recognition, encryption techniques and cloud computing technologies to ensure secure storage, transmission and processing of biometric data. The biometric information is encrypted before uploading it to the cloud, so unauthorised users or cloud providers cannot directly access sensitive personal information.

The system mainly comprises three modules, i.e., the Database Owner, User and Cloud Server. The biometric data is encrypted and handled by the database owner before being stored in the cloud. User sends biometric query requests for authentication. The cloud server processes encrypted queries to find matching biometric patterns without compromising security. This approach improves the system efficiency and privacy protection and reduces the risks of the conventional biometric authentication systems.

The project is developed using Java, JSP, JDBC, MySQL and networking technologies. Java offers a secure, platform-independent and object-oriented environment for building scalable applications. JDBC and MySQL are used for database connectivity and secure data management, and networking protocols are used to support communication between system modules.

In conclusion, this project shows that cloud-based biometric systems can provide secure authentication, efficient recognition, and strong privacy protection through the application of encryption and secure communication mechanisms. It offers a reliable approach to modern authentication mechanisms where data privacy and user trust are critical.

II. RELATED WORK

Numerous research works and existing systems are concerned with enhancing the efficiency, security and privacy protection of biometric recognition systems. Traditional biometric authentication methods were mainly based on storing biometric templates such as fingerprints, iris patterns, facial images and voice data in centralised databases. These systems had accurate user identification, but had major privacy and security limitations as sensitive biometric information can be exposed to attackers during storage or transmission.

Early biometric systems mainly emphasised recognition accuracy and did not consider privacy preservation a priority. These systems stored the biometric templates in plain form and were vulnerable to unauthorised access, data theft, replay attacks, and identity leakage. Then, cryptographic techniques and secure template protection methods were proposed by researchers to overcome these challenges. To preserve the confidentiality of the biometric data even in remote servers or cloud environments, encryption-based biometric systems were developed.

With the development of cloud computing, many biometric recognition systems began to use cloud servers to store and process biometric databases in the large scale. Cloud-based biometric systems increased scalability, flexibility, and accessibility, but they also raised new security issues, as cloud providers could potentially access sensitive user information. To solve this problem, secure cloud-assisted biometric recognition models have been proposed, in which biometric templates are encrypted before being uploaded to the cloud. These approaches reduced the risk of data leakage while retaining recognition efficiency.

Several existing works have also leveraged on searchable encryption and secure query processing techniques to perform biometric matching over encrypted data. In these systems, the user sends encrypted biometric queries to the cloud and the cloud performs matching operations without directly having access to the original biometric information. This concept has greatly improved the privacy and confidentiality of users in cloud based authentication systems. However, some of the previous methods have the disadvantages of high computational complexity, long processing time and low matching accuracy.

Machine learning and artificial intelligence techniques were also used by biometric recognition systems for optimising identification speed and accuracy. These methods improved pattern recognition capabilities in fingerprint, facial recognition and iris detection systems. At the same time, researchers concentrated on the implementation of secure communication protocols, access control mechanisms and data anonymisation techniques to enhance privacy protection.

The proposed project "Cognizant Biometric Recognition with Efficiency and Privacy Protection" is an extension of these existing research works where cloud computing, biometric authentication, encryption and secure query processing are integrated into one framework. The system guarantees that the biometric data is encrypted before storage and is securely handled during authentication. It offers separate modules for database owner, user and cloud server for controlled access and secure biometric matching. The method enhances recognition efficiency and data privacy and mitigates the risks of traditional biometric systems.

The project is implemented with Java, JDBC, networking technologies, and cloud-based communication, which further helps in secure data handling and platform-independent operation. The proposed system provides better security and efficient biometric identification in cloud environment compared to conventional biometric systems.

III.METHODOLOGY

The methodology of the project "Cognizant Biometric Recognition with Efficiency and Privacy Protection" is to provide secure biometric authentication, high efficiency and strong privacy preservation by using cloud computing and encryption techniques. The system has a well defined process that includes collection of biometric data, encryption, secure storage, query processing and user authentication. The whole system is divided into three big modules: Database Owner, User and Cloud Server. Each module performs some actions to make communication secure and biometric recognition accurate.

In the first step, the database owner collects biometric information from users like fingerprints, facial patterns, iris scans or other biometric traits. The biometric data is then stored in the cloud after being securely encrypted with strong encryption techniques. The encryption secures the biometric templates from unauthorised access and also prevents the attackers and the cloud providers from directly accessing the private user information. The encrypted protected biometric data is uploaded and stored securely in the cloud server.

When a user requires access to the system, or wants to authenticate himself, the user sends a biometric query request. To ensure data confidentiality during communication, the input biometric information is converted into an encrypted query before transmission. The encrypted query is received by the cloud server and secure matching operations are performed with the encrypted biometric templates stored in the database. The matching process is performed on encrypted data, thus the original biometric data is hidden during the authentication process.

The cloud server searches for the closest biometric pattern, and sends the encrypted outcome to the database owner. Then the database owner computes the similarity between the query data and the stored biometric data to correctly verify the user identity. If the biometric patterns match successfully, the user is authenticated and allowed to enter the system. This approach improves authentication accuracy and maintains user privacy and data leakage.

Java, JSP, JDBC, MySQL, and networking technologies are used for the implementation of the system. JDBC and MySQL are used to manage and connect to the database. Java provides a secure and platform independent environment for application development. Networking protocols establish the communication between user, cloud server and database owner modules. This system has a secure communication mechanism, an encrypted data transfer mechanism and an access control mechanism so that it can be more reliable and secure.

In conclusion, the proposed methodology provides secure biometric authentication, efficient cloud-based processing, and strong privacy protection by integrating encryption, secure communication and cloud computing technologies into a unified biometric recognition framework.

IV. SYSTEM ARCHITECTURE:

The system architecture of the project "Cognizant Biometric Recognition with Efficiency and Privacy Protection" is designed to provide secure biometric authentication using cloud computing and encryption mechanism . The architecture is constructed primarily around three main entities: Database Owner, User and Cloud Server. All these components work together to provide efficient biometric recognition while maintaining the privacy and confidentiality of the biometric information. The proposed architecture offers secured storage, encrypted communication, and accurate biometric matching in a cloud environment.

The architecture first phase consists of the Database Owner who is responsible to collect and manage the biometric data like fingerprints, facial patterns, iris scans and other biometric traits. The owner encrypts the biometric information and uploads it to the cloud server. Encryption protects sensitive biometric data from unauthorised access, when it is being stored and transmitted. The authentication process also gets the user requests and does the similarity verification results by the database owner.

The User Module is the one that asks to be authenticated by the system. The user submits biometric information as a query request when the user wants to access the system. The biometric query is converted into encrypted form before sending it out so that the confidentiality and privacy are maintained. The user interacts securely with the cloud server and the database owner to authenticate and identify themselves.

The Cloud Server Module plays a critical role in storing encrypted biometric templates and performing encrypted biometric query processing. The cloud server receives the encrypted query from the user and then performs the secure matching operations between the encrypted query and the encrypted biometric database. The server finds the most similar biometric pattern and sends back the encrypted matching result to the database owner without exposing the real biometric information. The architecture provides better scalability, storage efficiency and computational performance with a strong privacy protection.

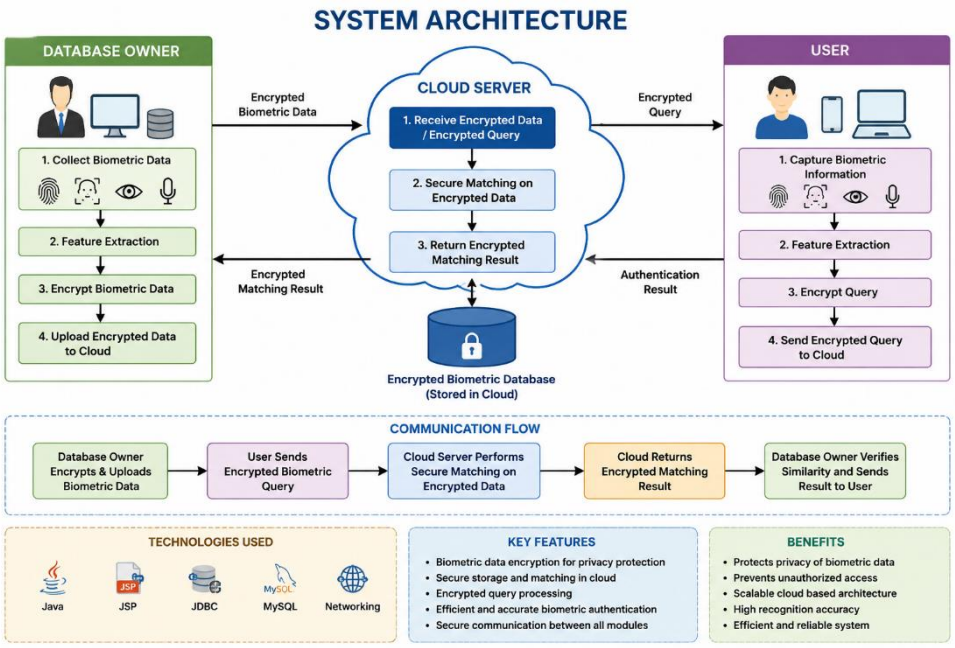
The system architecture also comprises secure communication channels, encryption mechanisms and database management components . The project is developed using Java, JSP, JDBC, MySQL and networking technologies. Java provides platform independence and security features and JDBC and MySQL provides database connectivity and data management. Networking protocols enable communication between all system modules in a secure way.

In summary, the proposed system architecture provides a reliable and secure cloud-based biometric recognition system that enables efficient authentication, encrypted biometric processing, and strong privacy preservation for users and organisations.

A. Overview:

The image depicts the system architecture of the Cognisant Biometric Recognition with Efficiency and Privacy Protection project. It shows the interaction between Database Owner, Cloud Server and User modules. The database owner collects the biometric data, encrypts it, and stores it in the cloud . The users send the encrypted biometric queries to authenticate themselves. The cloud server securely matches the encrypted data and securely returns authentication results. The architecture offers privacy protection, secure communication, efficient biometric recognition and reliable cloud-based authentication.

B. Architecture Diagram:



V. EXPERIMENTAL SETUP:

The experimental setup of the project "Cognizant Biometric Recognition with Efficiency and Privacy Protection" is designed to evaluate the performance, security and efficiency of the proposed biometric authentication system in a cloud environment. The system comprises hardware, software, database management, networking and encryption modules for the secure processing and authentication of biometric data. The system is implemented using Java technologies and cloud-based communication architecture for secure biometric recognition with privacy preservation.

The hardware configuration used for implementation is a normal computer system with Intel processor, minimum 4 GB RAM and sufficient storage capacity for biometric data and database operation. The software environment consists of Windows operating system, Java Development Kit (JDK), JSP, JDBC, Apache Tomcat Server and MySQL database server. The primary programming language is Java, due to its platform independence, security features, and object orientated architecture. Dynamic web pages and database connectivity are developed using JSP, JDBC and MySQL is used for secure storage of encrypted biometric information.

The experimental system consists of three main modules, namely, the Database Owner, the User, and the Cloud Server. In the first phase, the database owner feeds biometric data such as finger prints, face images or iris information into the system. The biometric data is kept in an encrypted form to keep it confidential and to prevent unauthorised access. The encrypted biometric templates are then stored in the cloud database to be securely retrieved and processed.

The user interface allows users to submit biometric query requests during the authentication process. The system encrypts the query and sends it to the cloud server over secure communication channels. The cloud server performs encrypted biometric matching operation without disclosing the original biometric information. Once the matching biometric template is found, the server sends the encrypted result back to the database owner. The database owner checks the similarity score and authenticates the user. This set up provides a secure biometric matching with better privacy protection and authentication accuracy.

The communication between the modules is configured by the TCP/IP communication protocols providing secure data transfer. The experimental setup comprises encryption algorithms, secure query processing and access control mechanisms to protect biometric information during transmission and

storage. The system further employs cloud storage techniques to improve the scalability, flexibility and efficiency of data management.

The experimental setup as a whole shows the real world implementation of a secure cloud based biometric recognition system that can provide efficient authentication, secure biometric processing, lower privacy risks and reliable user verification in distributed environments.

VI. RESULT AND DISCUSSION:

The proposed project "Cognizant Biometric Recognition with Efficiency and Privacy Protection" has been successfully implemented and tested in cloud based environment using Java, JSP, JDBC, MySQL and encryption techniques. The system was efficient in biometric authentication and improved privacy protection and secure communication between the database owner, user and cloud server modules. The experimental results indicate that the proposed framework can not only protect the biometric information but also achieve high recognition accuracy and authentication performance.

During the execution of the system, the user's identity information and biometric templates were encrypted as biometric information successfully and uploaded to the cloud database. The encryption mechanism ensured confidentiality in storage and transmission and prevented unauthorised access to sensitive biometric information. The cloud server efficiently processed encrypted biometric queries and performed secure matching operations without revealing the original biometric data. This greatly reduced the risk of privacy leaks and data exposure in the cloud environment.

In the user authentication process, several biometric queries were tested. The system successfully identified valid users by comparing encrypted biometric queries with encrypted biometric templates in the cloud database. The authentication results confirmed that the system achieved accurate biometric recognition with the user's privacy preserved. The encrypted query processing improved security and prevented attackers from obtaining the original biometric information in communication.

The cloud-based architecture improved scalability and storage efficiency by securely storing the biometric templates in a centralised cloud environment. Networking protocols and secure communication mechanisms were implemented to ensure reliable data transfer between the modules. The stable performance of the system and effective handling of biometric records have been ensured by the integration of java technologies, JDBC connectivity and MySQL database management.

The discussion of the results shows that the suggested system provides the better security and privacy protection than the traditional biometric authentication systems in which the biometric data is stored in plain form. The encryption-based technique was found to minimise the risk of unauthorised access, replay attacks, and leakage of biometric data. Moreover, the computational overhead did not increase significantly by the secure matching mechanism, and the recognition speed and authentication accuracy were still efficient.

Overall, the results show that the proposed biometric recognition system is robust, secure and efficient for cloud-based authentication applications. The system efficiently integrates the biometric recognition, encryption and cloud computing technologies for the purpose of privacy-preserving authentication with better security and performance.

VII. CONCLUSION:

Under the project "Cognizant Biometric Recognition with Efficiency and Privacy Protection", a secure and efficient biometric authentication system integrated with cloud computing and encryption technologies is presented in this paper. The proposed system overcomes the major challenges of the traditional biometric systems like privacy leakage, unauthorised access and insecure storage of biometric information. The proposed system ensures strong confidentiality and secure user authentication by encrypting the biometric data before storing and processing it in the cloud.

The system is divided into individual modules for the Database Owner, User and Cloud Server, which facilitates secure communication and dependable biometric matching. The cloud server efficiently computes the encrypted biometric queries and returns the secure authentication results without leaking any sensitive biometric templates. This approach improves recognition accuracy and privacy preservation, and reduces risks associated with cloud-based biometric systems.

Java, JSP, JDBC, MySQL and networking technologies provide stable and scalable platform for implementing secure biometric applications. The system illustrates efficient storage management, safe data transmission and reliable authentication performance in distributed cloud environment. Moreover, the encryption mechanisms and the secure query processing methods are employed to protect biometric information from attackers, replay attacks and unauthorised users.

In summary, the proposed biometric recognition framework provides efficient authentication, enhanced security, strong privacy protection, and effective cloud-based biometric data management. The project shows that the combination of biometric recognition with encryption and cloud technologies can be an effective and safe solution for modern authentication systems in organisations, industries and online services.

VIII.REFERENCES:

1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Education, 2017.
3. Ian Sommerville, Software Engineering, 10th Edition, Pearson Education, 2017.
4. Anil K. Jain, Arun Ross, and Salil Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4–20, 2004.
5. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer Science & Business Media, 2006.
6. Ratha N. K., Connell J. H., and Bolle R. M., “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” IBM Systems Journal, Vol. 40, No. 3, pp. 614–634, 2001.
7. Boneh D. and Franklin M., “Identity-Based Encryption from the Weil Pairing,” SIAM Journal on Computing, Vol. 32, No. 3, pp. 586–615, 2003.
8. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” IEEE INFOCOM, pp. 525–533, 2010.
9. A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” Proceedings of IEEE International Symposium on Information Theory, pp. 408–408, 2002.
10. P. Tuyls and J. Goseling, “Capacity and Examples of Template-Protecting Biometric Authentication Systems,” Biometric Authentication Workshop, Springer, pp. 158–170, 2004.
11. Sun Microsystems, Java 2 Platform Standard Edition Documentation, Oracle Corporation.
12. Herbert Schildt, Java: The Complete Reference, 9th Edition, McGraw-Hill Education, 2014.
13. Deitel & Deitel, Java How to Program, Pearson Education, 2015.
14. Jason Hunter and William Crawford, Java Servlet Programming, O’Reilly Media, 2001.
15. Elmasri R. and Navathe S. B., Fundamentals of Database Systems, 7th Edition, Pearson Education, 2016.