2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

SECURE CRYPTO-BIOMETRIC SYSTEM FOR CLOUD COUMPTING

Mr. N. Chandiraprakash[1],m ravindranath[2],chevva mahesh babu[3],dwarapudi lakshmi deepika[4],neeraj kumar bomma[5],mohd aqibuddin[6]

[1]Assistant Professor,department of information technology,malla reddy institute of engineering and technology(autonomous),dhulapally,secundrabad

[2,3,4,5,6]UG Students,department of information technology,malla reddy institute of engineering and technology(autonomous),dhulapally,secundrabad

ABSTRACT

Cloud computing has achieved maturity, and there is a heterogeneous group of providers and cloud-based services. However, significant attention remains focused on security concerns. In many cases, security and privacy issues are a significant barrier to user acceptance of cloud computing systems and the advantages these offer with respect to previous systems. Biometric technologies are becoming the key aspect of a wide range of secure identification and personal verification solutions, but in a cloud computing environment they present some problems related to the management of biometric data, due to privacy regulations and the need to trust cloud providers. To overcome those problems in this paper, we propose a cryptobiometric system applied to cloud computing in which no private biometric data are exposed.

I.INTRODUCTION:

Cloud computing is a trend in application architecture and development, as well as a new business model. The success of many service providers, with Amazon as a remarkable example, has demonstrated that the model can be applied to a wide variety of solutions, covering the different levels defined in the cloud paradigm (SaaS, PaaS and IaaS). We can consider that cloud computing is at a mature stage, although there remain some limitations and challenges. Cloud computing brings important benefits for organizations that outsource data, applications, and infrastructure, at the cost of delegating data control. The information is processed in computers that the users do not own, operate, or manage. In this scenario, the user does not know how the provider handles the information, and therefore a

high level of trust is needed. The lack of control over physical and logical aspects of the system imposes profound changes in security and privacy procedures.

PURPOSE

The purpose of the project is to develop a secure crypto-biometric system for cloud computing. Cloud computing has become increasingly popular, enabling users to store and access their data remotely. However, security concerns have also risen due to the sensitive nature of the data being stored and transmitted. This project aims to address these concerns by combining the power of cryptography and biometric authentication.

The system will employ advanced cryptographic algorithms to ensure the confidentiality, integrity, and authenticity of the data stored in the cloud. These algorithms will encrypt the data before transmission and decrypt it upon retrieval, protecting it from unauthorized access or tampering. Additionally, the system will utilize biometric authentication techniques, such as fingerprint or iris scanning, to verify the identity of users accessing the cloud resources.

By integrating cryptography and biometrics, the system will provide a robust and multi-layered security framework. It will prevent unauthorized access to the cloud infrastructure and ensure that only authenticated individuals with verified biometric credentials can interact with the data stored in the cloud. This approach eliminates the risks associated with traditional password-based authentication systems, such as password cracking or sharing.

Overall, the secure crypto-biometric system for cloud computing aims to enhance data security, privacy, and access control in the cloud environment. It provides a reliable and efficient solution for individuals and organizations seeking to protect their sensitive information while leveraging the benefits of cloud computing.

SCOPE

The scope of the project is to develop a secure crypto-biometric system specifically designed for cloud computing environments. The objective is to enhance the overall security of cloud-based applications by combining cryptographic techniques with biometric authentication.

The system will employ state-of-the-art encryption algorithms to protect the confidentiality and integrity of data stored in the cloud. Additionally, it will leverage biometric authentication methods, such as fingerprint or iris recognition, to ensure

secure access to the cloud resources. By integrating these two powerful security measures, the project aims to provide a robust and multi-layered defense against unauthorized access and data breaches.

The system will be designed to seamlessly integrate with existing cloud platforms, allowing users to securely store and access their data without compromising usability. It will also incorporate mechanisms for secure key management, ensuring that cryptographic keys used for data encryption are properly stored and protected.

The project will involve developing and implementing novel cryptographic protocols and biometric authentication algorithms. Extensive testing and evaluation will be conducted to ensure the system's effectiveness and resilience against various attack vectors. Furthermore, the project will consider scalability and performance aspects to ensure that the proposed solution can handle large-scale cloud deployments.

The final deliverable will be a comprehensive and secure crypto-biometric system that can be readily integrated into cloud computing environments, providing enhanced security for sensitive data stored and processed in the cloud.

II.LITERATURE REVIEW

1.Secure crypto-biometric system for cloud computing,David González Martínez; Francisco Javier González Castaño; Enrique Argones Rúa; José Luis Alba Castro;Cloud computing has achieved maturity, and there is a heterogeneous group of providers and cloud-based services. However, significant attention remains focused on security concerns. In many cases, security and privacy issues are a significant barrier to user acceptance of cloud computing systems and the advantages these offer with respect to previous systems. Biometric technologies are becoming the key aspect of a wide range of secure identification and personal verification solutions, but in a cloud computing environment they present some problems related to the management of biometric data, due to privacy regulations and the need to trust cloud providers. To overcome those problems in this paper, we propose a cryptobiometric system applied to cloud computing in which no private biometric data are exposed.

2.Cognitive and Biometric Approaches to Secure Services Management in Cloud-Based Technologies,Marek Ogiela; Lidia Ogiela,This article describes new ideas for applying security procedures to data and service management in cloud and fog computing. Management in cloud computing is presented in connection with cognitive systems supporting management tasks and securing important data. The application of cognitive and biometric features allows creation of personalized procedures oriented at particular users or a group of protocol participants.

III.EXISTING SYSTEM:

the data are stored in the user infrastructure, information location and protection mechanisms are known in detail. In contrast, a characteristic of public cloud computing services is that the user is completely unaware of data location. This makes it impossible to ensure that national compulsory regulations are met. For example, European data protection laws may impose extra constraints on the handling and processing of data that are transferred to the USA, so the use of Amazon S3 resources to store biometric templates could infringe the law. Several techniques have been proposed for biometric template protection. Among them, cancelable biometrics [10] is one of the most promising. It satisfies a double goal: i) unrecoverability of the original biometric data from the stored biometric template (non-invertibility), and ii) the issue of a new biometric template when an existing template is compromised (renewability).

IV.PROPOSED SYSTEM:

In the proposed schema, once a large database with sample acquisitions has been collected, an UBM can be trained. We propose the training methodology in Figure 3 (the addition of new UBMs) to improve the flexibility and security of our system. To train a new UBM, computing resources are provided by virtual machines hosted in Amazon EC2. The administration application requests from Amazon EC2 the required virtual machines automatically, using the API it provides. The training application and the new UBM are loaded and executed in the machines in a distributed way to reduce computation time. Speedup is possible due to the high

International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal
2581-4575

parallelizability of the calculus performed on biometric data.

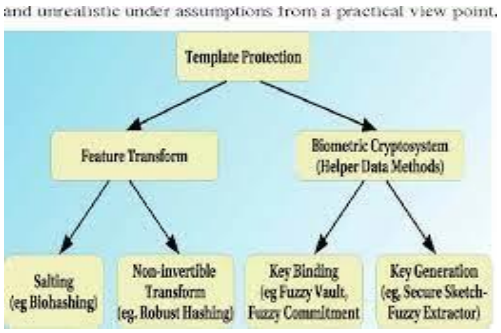


Fig1. System Diagram

V.FUNCTIONAL REQUIREMENTS

The functional requirements for the project "Secure Crypto-Biometric System for Cloud Computing" can be summarized as follows:

1. **User Authentication:** The system should support biometric authentication mechanisms, such as fingerprint or iris recognition, to verify the user's identity before granting access to cloud resources.

2. **Data Encryption:** All data transmitted between the user and the cloud should be encrypted using strong cryptographic algorithms to ensure confidentiality.

3. **Secure Key Management:** The system should provide a secure key management mechanism to generate, store, and distribute cryptographic keys used for data encryption and decryption.

4. **Multi-Factor Authentication:** In addition to biometric authentication, the system should support other factors, such as passwords or tokens, to provide multi-factor authentication and enhance the overall security of the system.

5. **Access Control:** The system should enforce fine-grained access control policies to restrict user access to specific cloud resources based on their roles, privileges, or other defined criteria.

6. **Secure Communication Channel:** The system should establish a secure communication channel between the user and the cloud provider to prevent eavesdropping and ensure data integrity.

7. **Intrusion Detection and Prevention:** The system should incorporate mechanisms to detect and prevent unauthorized access attempts or suspicious activities within the cloud environment.

8. **Audit and Logging:** The system should maintain comprehensive logs of user activities, system events, and access

attempts to facilitate auditing, monitoring, and forensic analysis.

By meeting these functional requirements, the Secure Crypto-Biometric System for Cloud Computing aims to provide a secure and reliable platform for users to securely access and utilize cloud resources while protecting their sensitive data.

VI.NON-FUNCTIONAL REQUIREMENTS:

NON-FUNCTIONAL REQUIREMENT (NFR) specifies the quality attribute of a software system. They judge the software system based on Responsiveness, Usability, Security, Portability and other non-functional standards that are critical to the success of the software system. Example of nonfunctional requirement, “how fast does the website load?” Failing to meet non-functional requirements can result in systems that fail to satisfy user needs. Non- functional Requirements allows you to impose constraints or restrictions on the design of the system across the various agile backlogs. Example, the site should load in 3 seconds when the number of simultaneous users are> 10000. Description of non-functional requirements is just as critical as a functional requirement.

- Usability requirement
- Serviceability requirement
- Manageability requirement
- Recoverability requirement
- Security requirement

VII.PERFORMANCE REQUIREMENTS

The project "Secure Crypto-Biometric System for Cloud Computing" aims to develop a robust and efficient solution that combines cryptography and biometric authentication to enhance the security of cloud computing environments. The system will provide a multi-layered approach to safeguard sensitive data and ensure the privacy and integrity of user information.

To achieve this, the system must meet certain performance requirements. First and foremost, it should have low latency to ensure real-time response and smooth user experience. This is crucial in cloud computing environments where users expect quick and seamless access to their data and applications.

Additionally, the system should be scalable to accommodate a large number of users and handle varying workloads effectively. As cloud computing is characterized by its ability to serve multiple users concurrently,

the solution should be capable of handling high traffic and requests without compromising performance.

Moreover, the system should demonstrate high throughput to efficiently process cryptographic operations and biometric authentication tasks. This ensures that the system can handle a significant number of transactions simultaneously without creating bottlenecks. Furthermore, the solution should have low computational overhead to minimize resource consumption and optimize energy efficiency. It should be designed to efficiently utilize the available computing resources in the cloud environment, maximizing cost-effectiveness. Finally, the system should exhibit a high level of accuracy and reliability in biometric authentication to ensure the security of user identities. The biometric algorithms employed should have low false acceptance and false rejection rates, providing a robust and dependable authentication mechanism.By meeting these performance requirements, the Secure Crypto-Biometric System for Cloud Computing can deliver a secure, efficient, and user-friendly solution that enhances the overall security posture of cloud-based applications and services.

VIII.SDLC METHODOLOGIES

The Secure Crypto-Biometric System for Cloud Computing follows a specific Software Development Life Cycle (SDLC) methodology to ensure effective and efficient development, testing, and deployment of the system. The chosen SDLC methodology for this project is the Agile methodology, which emphasizes iterative and incremental development, collaboration, and flexibility.

The Agile methodology is well-suited for complex and evolving projects like the Secure Crypto-Biometric System. It allows for the frequent delivery of working software increments, enabling early feedback and continuous improvement. The development process consists of short iterations called sprints, typically lasting one to four weeks, where the team focuses on delivering a set of prioritized features.

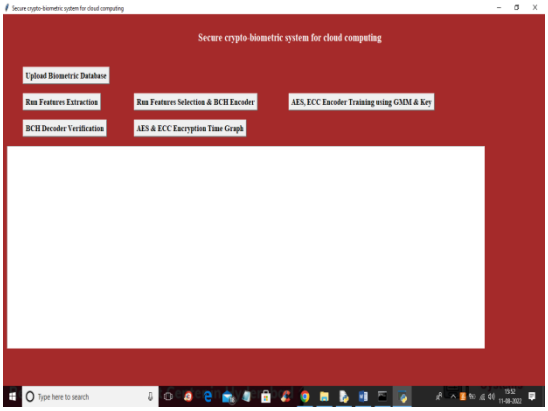
The Agile methodology encourages close collaboration between the development team, stakeholders, and end-users. Regular meetings, such as daily stand-ups and sprint reviews, facilitate communication, gather feedback, and ensure alignment with

International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal
2581-4575

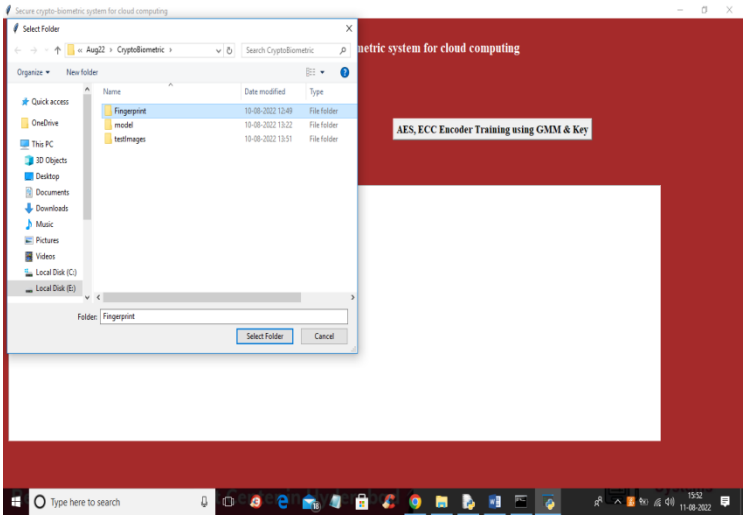
project goals. This iterative approach enables the team to adapt to changing requirements and make necessary adjustments throughout the development lifecycle.

Within each sprint, the team follows a set of core practices, including continuous integration, automated testing, and regular demonstrations of working software. These practices ensure that the system remains stable, reliable, and secure throughout the development process. The team also conducts thorough testing, including functional, performance, and security testing, to address potential vulnerabilities and ensure the robustness of the system.

The Secure Crypto-Biometric System for Cloud Computing project adheres to the Agile methodology to deliver a secure, reliable, and user-friendly system that meets the requirements of cloud-based biometric authentication. This methodology's iterative and collaborative nature enables the development team to adapt to evolving needs, mitigate risks, and deliver a high-quality solution within the specified timeframe.

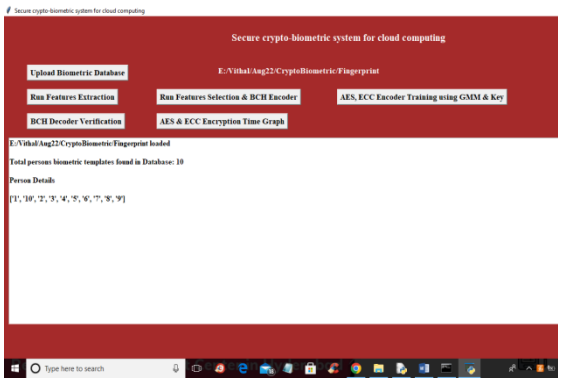


In above screen click on ‘Upload Biometric Database’ button to upload biometric data and get below output

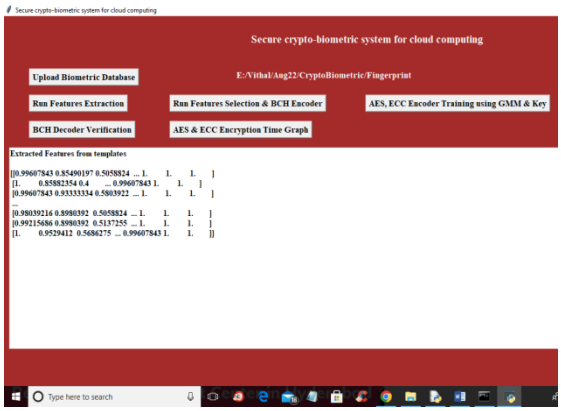


In above screen selecting and uploading Finger biometric images dataset and then click on ‘Select Folder’ button to load database and get below output

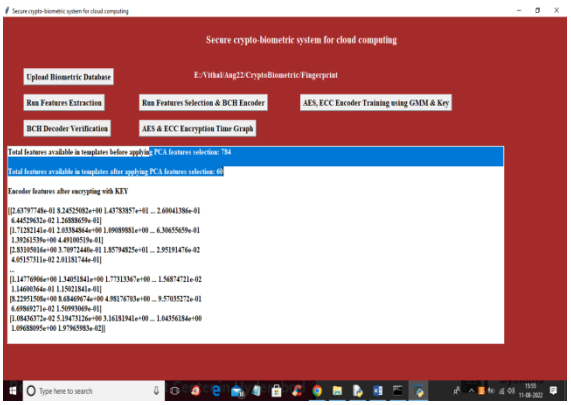
International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal



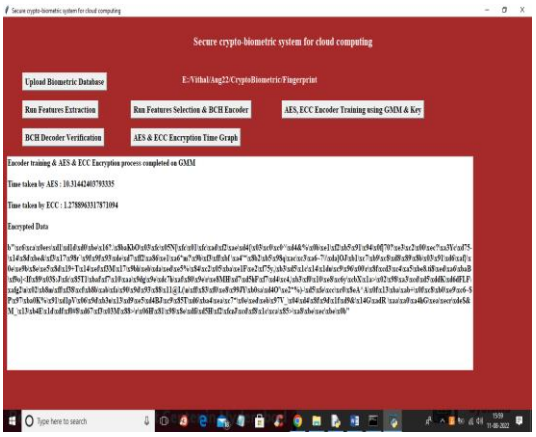
In above screen we can see database loaded and we can see it contains biometric template of 10 different persons and now click on 'Run Features Extraction' button o extract features from templates and get below output



In above screen features extracted and now click on 'Run Features Selection & BCH Encoder' button to select features from extracted features

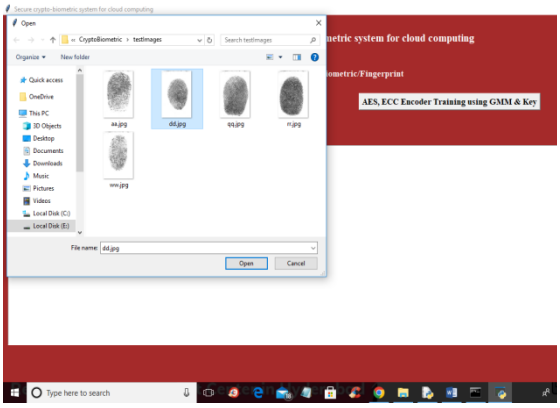


In above screen before applying PCA features selection algorithm, we have 784 features and then PCA select 60 important features out of it and now click on 'AES, ECC Encoder Training using GMM & Key' button to encode features and then train GMM and this GMM will get encrypted using ECC and AES algorithms and then will get below output

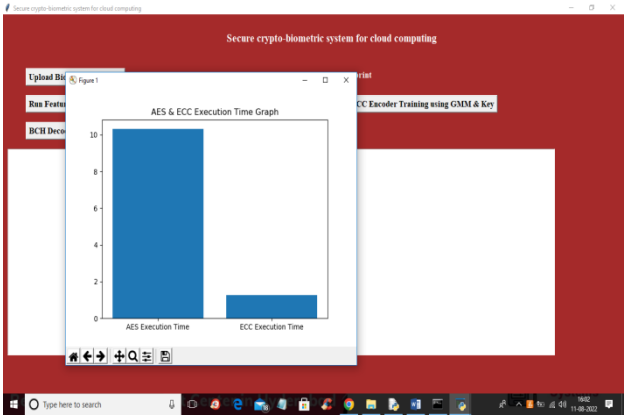


In above screen GMM is encrypted and AES took 10.31 seconds and ECC tool 1.2 seconds and then we are seeing GMM encrypted data and now click on 'BCH Decoder Verification' button to upload template and get verification output

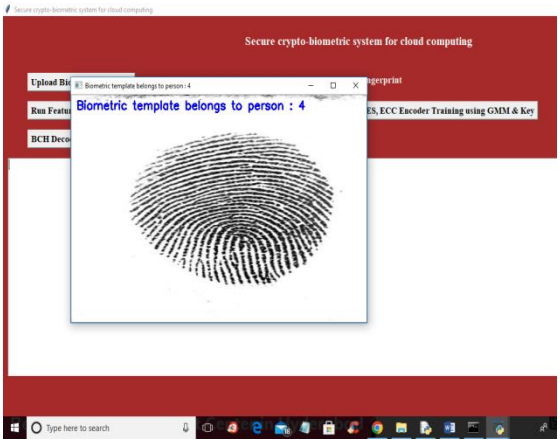
International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal



In above screen selecting and uploading finger template and then click on 'Open' button to get below output



In above graph x-axis represents encryption algorithm names and y-axis represents execution time and in both algorithms ECC took less execution time.



In above screen template identified or belongs to person 4 and now click on 'AES & ECC Encryption Time Graph' button to get below graph

CONCLUSION

In conclusion, the development of a secure crypto-biometric system for cloud computing offers a promising solution to address the growing concerns regarding data privacy and security. This innovative system combines the strength of cryptographic techniques with the unique characteristics of biometric authentication, resulting in a robust and reliable method for safeguarding sensitive information in cloud environments.

By leveraging cryptographic algorithms, the system ensures that data transmitted to and stored in the cloud remains encrypted and inaccessible to unauthorized individuals. This provides a solid foundation for protecting the confidentiality

and integrity of user data throughout the cloud computing process.

Additionally, the integration of biometric authentication adds an extra layer of security by verifying the identity of users based on their unique physiological or behavioral traits. This mitigates the risks associated with password-based authentication, such as weak passwords or credential theft, significantly reducing the chances of unauthorized access to sensitive data.

The secure crypto-biometric system not only enhances data security but also offers convenience and efficiency to users. By utilizing biometric characteristics like fingerprints or facial recognition, users can seamlessly authenticate themselves without the need to remember complex passwords, leading to a streamlined and user-friendly experience.

Overall, the implementation of a secure crypto-biometric system for cloud computing addresses critical security concerns and ensures the protection of sensitive data. It paves the way for a more secure and trustworthy cloud computing environment, instilling confidence in users and organizations alike.

REFERENCES

[1] A. A. M. Abd Hamid, N. and A. Izani. Extended cubic b-spline interpolation method applied to linear two-point boundary value problem. World Academy of Science, 62, 2010.

[2] T. Acharya. Median computation-based integrated color interpolation and color space conversion methodology from 8-bit bayer pattern rgb color space to 24-bit cie xyz color space, 2002. US Patent 6,366,692.

[3] A. F. Agarap. An architecture combining convolutional neural network (cnn) and support vector machine (svm) for image classification. arXiv preprint arXiv:1712.03541, 2017.

[4] A. Ben-Hur and J. Weston. A user's guide to support vector machines. In Data mining techniques for the life sciences, pages 223– 239. Springer, 2010.

[5] S. Bianco, F. Gasparini, A. Russo, and R. Schettini. A new method for rgb to xyz transformation based on pattern search optimization. IEEE Transactions on Consumer Electronics, 53(3):1020–1028, 2007.

[6] E. Bisong. Google colaboratory. In Building Machine Learning and Deep Learning Models on Google Cloud Platform, pages 59–64. Springer, 2019.

[7] A. P. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. Pattern recognition, 30(7):1145– 1159, 1997.

[8] S. A. Burney and H. Tariq. K-means cluster analysis for image segmentation. International Journal of Computer Applications, 96(4), 2014.

[9] M. A. Chandra and S. Bedi. Survey on svm and their application in image classification. International Journal of Information Technology, pages 1–11, 2018.

[10] L. de Oliveira Martins, G. B. Junior, A. C. Silva, A. C. de Paiva, and M. Gattass. Detection of masses in digital mammograms using kmeans and support vector machine. ELCVIA Electronic Letters on Computer Vision and Image Analysis, 8(2):39–50, 2009.