JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CRYPTO BIOMETRIC SYSTEM FOR CLOUD

R. Siddharth Goud[1], B. Yuvraj Singh[2] B.Puja[3], Mrs. Sakina H.Sayyed[4]

[1,2,3]B. Tech Student, Department of CSE-Artificial Intelligence & Machine Learning, CMRCET, Hyderabad, Telangana [4]Assistant Professor, Department of CSE- Artificial Intelligence & Machine Learning, CMRCET, Hyderabad, Telangana

Abstract : With a diverse range of cloud service providers and cloud-based offerings, cloud computing has reached a mature state. Security issues, however, continue to receive a lot of attention. Users' willingness to embrace cloud computing systems and their benefits over older systems is frequently hampered by concerns about security and privacy. Need to trust cloud providers due to privacy laws, biometric technologies are increasingly becoming the essential component of many secure identity and personal verification systems. Yet in the context of cloud computing, they pose certain management challenges for biometric data. In this research, we present a crypto biometric system that is applied to public cloud computing and ensures that zero private biometric data is accessible in order to address those issues.

***Keywords* – Cloud Computing, Biometric System, BCH Encoder & Decoder, Machine Learning**

I. INTRODUCTION

A new business model and trend within application design and development is cloud computing. This idea is applicable across various solutions, encompassing the different layers outlined in the cloud computing paradigm (SaaS, PaaS, and IaaS). This is evident in the achievements of many service providers, with Amazon being a prominent illustration. Even though there are still certain restrictions and difficulties, we can say the cloud computing has reached a mature stage. At the expense of giving up control over data, cloud computing offers significant advantages to businesses that outsource infrastructure, apps, and data. Computers that are not owned, operated, or managed by the users process the information. A high degree of trust is required in this situation because the user is unaware of how the supplier handles the information. Significant adjustments must be made to security and privacy protocols because to the absence of control over the system's logical and physical components. As of right now, service level agreements pertaining to security are non-existent between users and providers. Our research focuses on suitable security measures that might satisfy the traditional systems' legal requirements. Biometrics have been the focus of much research in recent years, and their security applications are becoming increasingly apparent. Biometric technology and cloud computing together create new avenues for application and study in cloud data protection. Nonetheless, considering the sensitive nature the biometric data, biometric templates need to be safe to even cloud service providers. Due to the difficulties of updating personal data in the same way, this requirement is more crucial than it is for alphanumerical passwords.

II. RELATED WORK

Outsourcing computation without outsourcing control.

The attractiveness of cloud computing lies in its cost-effectiveness and versatility, making it a highly appealing field in today's technology landscape. This perception views cloud computing as a fresh approach to IT procurement is eventually going to be jeopardized by serious, enduring worries about the technology, which are preventing progress despite the recent upsurge in activity and enthusiasm. We describe the issues and how they affect adoption in this study. More importantly, we outline how the convergence of current research directions can potentially address many of the issues preventing widespread implementation. To be more specific, we contend that living in the cloud can be more useful from a business intelligence perspective than the isolated option that is more prevalent now, provided that research into trusted computing and computation-supporting encryption continues.

Creating a system for secure, scalable, and detailed data access control within cloud computing.

Computing, A fresh perspective in the realm of computing called "cloud computing" allows computer infrastructure resources to be made available as online services. Even though this paradigm appears to be rather promising, Sharing sensitive data on cloud servers outside of the trusted domain of data owners introduces new challenges in access control and data security. To safeguard such data from untrusted servers, existing systems often employ cryptographic methods and restrict access to decryption keys to authorized users, do not scale effectively since they unavoidably place, When implementing fine-grained data access control, there is a notable computational burden placed on the data owner for managing data and distributing keys. This paper addresses the challenge of simultaneously ensuring scalability and maintaining data secrecy in access control, which is a complex open problem by enabling the data owner to delegate the majority of computational tasks related to fine-grained data access control to untrusted cloud servers without disclosing the actual data, all while establishing and implementing access policies based on data attributes. We accomplish this by taking advantage of and combining proxy re-encryption, lazy re-encryption, and attribute-based encryption (ABE) in a unique way. Important features of our suggested system include user secret key accountability and user access privilege confidentiality. A thorough analysis demonstrates that, under current security models, our suggested technique is both provably safe and extremely efficient.

Ensuring Cloud Computing Data Storage Security

It has been suggested that cloud computing will represent the next evolution of IT enterprise architecture. Cloud computing shifts the use of Software and databases are moved to large data sites, where managing information and services might not be straightforward. However, this is not entirely reliable compared to traditional systems, which have well-established physical, logical, and personnel controls for IT services. Special quality presents a number of novel and poorly understood security challenges. This article points on the security of data storage in the cloud, which has consistently been a vital aspect of service quality. We provide an efficient and adaptable distributed system with two key features that differs from its predecessors in order to guarantee the accuracy of information stored by users. Our system in the cloud achieves both storage correctness assurance and data error localization by employing homomorphic tokens with distributed verification on erasure-coded data. This includes identifying misbehaving servers. The novel approach, in contrast to most previous works, also provides data update, deletion, and add, among other performing dynamic operations on data blocks securely and efficiently. A thorough examination of security and performance reveals that the suggested plan is incredibly effective and resistant to malicious data alteration, server collusion, and Byzantine failure.

Designing Cloud Services with Data Protection in Mind: Proceedings of the Inaugural International Conference on Cloud Computing

The Cloud is a very new idea and so it is predictable since information assurance, safety of data, network privacy and security issues have yet been fully addressed. This study aims to prevent the costs related to adding safety as an afterthought by starting the process of incorporating data protection policies in clouds from the beginning. Our first approach is to describe a new capability maturity model and look at cloud maturity form an enterprise level perspective. With the use of this model, we investigate privacy controls in a business cloud deployment and identify potential areas for data protection control design as cloud exploitation advances. We illustrate how design patterns could be used to provide such controls. Lastly, we discuss the potential application of Service Level Agreements (SLAs) to guarantee the support of third-party vendors for these controls.

III. METHODOLOGY

To implement this project author has designed following modules

1.Upload Biometric Database: using this module we will upload biometric templates database to application

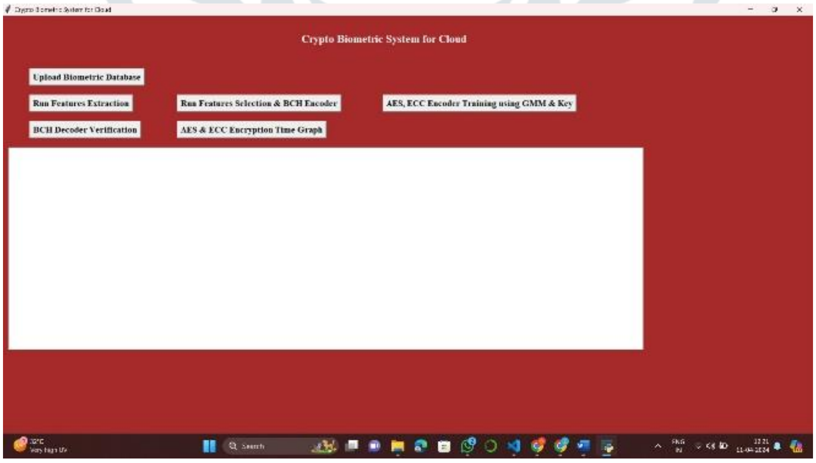
2.Run Features Extraction: using this module we will extract features from templates

3.Run Features Selection & BCH Encoder: in this module using PCA we will select features and then encode the features

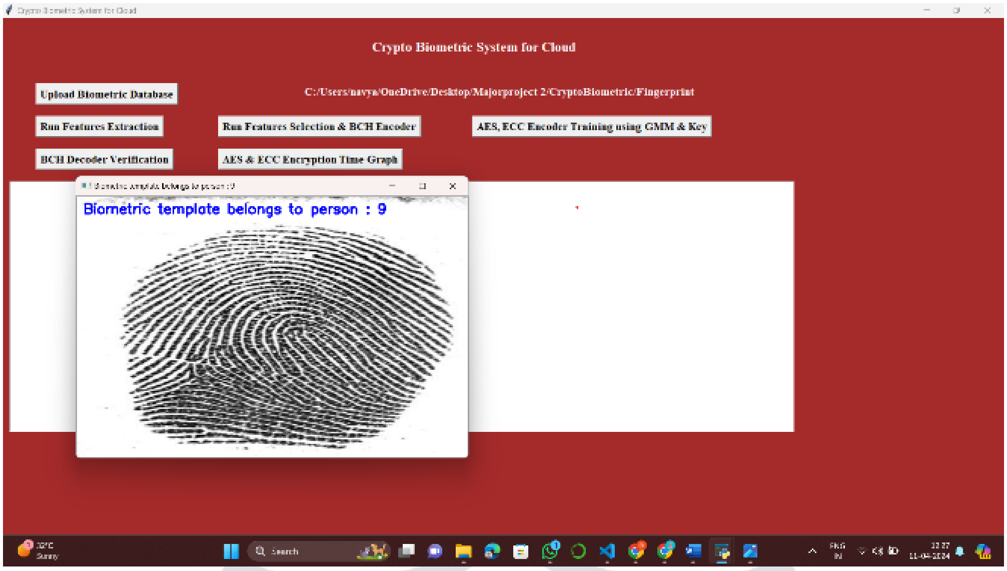
4.Encoder Training using GMM & Key: encoded features will key get trained with GMM

5.BCH Decoder Verification: using this module we will upload test image and then decode and perform verification

IV. RESULTS


Crypto Biometric System for Cloud
Crypto Biometric System for Cloud
Upload Biometric Database
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph

In above screen click on ‘Upload Biometric Database’ button to upload database and get below screen.



Crypto Biometric System for Cloud

C:/Users/navya/OneDrive/Desktop/Majorproject 2/CryptoBiometric/Fingerprint

Biometric template belongs to person : 9

Upload Biometric Database
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph

In above screen we can see uploaded template belongs to person 4 and similarly you can upload and verify other templates.

V. CONCLUSION

Our proposal is a workable and secure cryptography system designed to protect sensitive information in cloud computing settings. Accurate and secure information access is made possible with biometric identification. Our methodology guarantees that neither the biometric data of the user nor the outcome if the biometric secret matching identification is known by the cloud, which is a significant distinction from existing biometric schemas. Our model's lack of a direct matching procedure strengthens its security and improves its suitability for legal compliance. We have put forth a technique that enables a verifier to verify a user's identity while keeping the verifier from discovering any personal biometric data. To enhance security, a training system has been created to broaden the range of schema models for third-party cloud applications utilizing this standard. System efficiently completes computationally demanding tasks by utilising cloud resources. A traditional private as well as public key technique is used for authentication. This makes it possible for the system to utilise all of the infrastructures and solutions built around certifying authority and that particular kind of cryptography. Our crypto biometric system can be made better in a few areas. The amount of time needed for processing the use of biometric data within a client application poses a significant limitation. It may result in complex model combinations. result in processing user biometric data taking too long (a few seconds for a 16-UBM system, as previously indicated), which would impact reaction times and the interactive Ness of apps that use our schema. It is necessary to do a thorough inquiry in order to improve process time. Cloud computing resources could be quite helpful in this regard. As a result, future research will focus on finding a safe method of processing biometric data that keeps it private and unavailable to outside parties, including the cloud provider. A whole Software as a Service at last It is possible to create a solution that offers our approach's capabilities as a service.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing, Proceedings of the 29th conference on Information communications, IEEE INFOCOM 2010: 534-542, San Diego, CA, USA, Mar 2010.

[2] Vidhya, V., Kiran, A., Bhaskar, T., Boddupalli, S.” Machine Learning-based Reduction of Food Remains and Delivery of Food to the Needy”,Proceedings of the 2023 2nd International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2023, 2023, pp. 878–882

[3] Reddy, A.R., Narendar, Ch., Srinu, K., ...Reddy, R.V., Sruthi, P.” COVID 19 Patient Recognition and Prevention Utilizing Machine Learning and CNN Model Techniques”,5th IEEE International Conference on Cybernetics, Cognition and Machine Learning Applications, ICCCMLA 2023, 2023, pp. 677–686

[4] Sasi Bhanu, J., Kamesh, D.B.K., Durga Bhavani, B., Saidulu, G.” An Architecture on Drome Agriculture IoT Using Machine Learning”,Cognitive Science and Technology, 2023, Part F1493, pp. 635–641

[5] Y Ambica, Dr. N. Subhash Chandra, A Cascaded Deep Network for Abnormal Region Extraction from MR Brain Images. International Journal of Grid and Distributed Computing. Vol. 13, No. 2, (2020), pp. 1554-1563

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, Ensuring data storage security in Cloud Computing. 17th International Workshop on Quality of Service, Iwo 2009: 1-9, Charleston, SC, USA, Jul 2009.

[7] P. Tuyls, E. Verbosity, J. Gooseling, and D. Dentine, Privacy protecting biometric authentication systems: an overview, EUSIPCO 2004: XII European Signal Processing Conference: 1397-1400, Vienna, Austria, Sep 2004.

[8] A.K. Jain, K. Nandakumar, A. Nagar, Biometric Template Security, EURASIP Journal on Advances in Sign. Proc., Special Issue on Biometrics: 113:1–113:17, 2008.

[9] N. Ratha, S. Chikara J. H. Connell, R. M. Bolle, Generating Cancellable Fingerprint Templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4): 561-572, 2007.

[10] E. Maiorana, P. Campisi, J. Fierer, J. Ortega-Garcia, A. Neri, Cancellable templates for sequence-based biometrics with application to online signature recognition, IEEE Transactions on Systems, Man and Cybernetics Part A, 40(3): 525-538, 2010.

[11] D.A. Reynolds, T.F. Quintieri, R.B. Dunn, Speaker verification using adapted gaussian mixture models, Digital Signal Processing, 10(1-3): 19-41, 2000.

[12] P. Kenny, G. Bouziane, P. Dumouchel, Eigen voice Modelling with Sparse Training Data, IEEE Transactions on Speech and Audio Processing, 13(3): 345-354, 2005.

[13] A. Juels, M. Wattenberg, A Fuzzy Commitment Scheme, CCS99 Sixth ACM Conference on Computer and Communication Security: 28- 36 Singapore, India, Nov 1999.

[14] P. Tuyls, A. Akkermans, T. Keven Aar, G.J. Shrien, A. Bazen, R. Veldhuis, Practical biometric template protection system based on reliable components, Audio- and Video-Based Biometric Person Authentication (AVBPA): 436-446, Hilton Rye Town, NY, USA, Jul 2005.