DOI: https://doi.org/10.61841/turcomat.v15i3.14776
Turkish Journal of Computer and Mathematics Education (TURCOMAT) ISSN: 3048-4855

Vol.15 No.3(2024),35-44

A Secure Crypto-Biometric System Utilizing GMM Encoder and BCH

Ms. Sanjeevini [1], B. Ashraya [2], G. Aparnika[3], M. Akshitha[4]

[1] Assistant Professor, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

[2] [3] [4] Student, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

ABSTRACT:

Now that cloud computing has reached maturity, a diverse array of providers and services are available in the cloud. On the other hand, security issues continue to receive a lot of focus. Despite the many benefits of cloud computing, users are hesitant to embrace the technology due to concerns about their security and privacy. While biometric technologies are rapidly becoming an integral part of many secure identification and personal verification solutions, they do pose certain challenges when stored in the cloud owing to privacy regulations and the requirement to have faith in cloud providers when handling biometric data. In this work, we offer a crypto biometric system that can be used with cloud computing to solve these issues. This system ensures that no private biometric data is revealed.

INTRODUCTION

Cloud computing is both a new way of doing business and an emerging trend in the design and development of applications. A number of service providers' successes—Amazon included—have shown that the approach is applicable to a broad range of solutions, spanning the multiple tiers of the cloud paradigm (SaaS, PaaS and IaaS). Cloud computing has reached a certain level of maturity, while it still faces some constraints and obstacles. Businesses that outsource their data, apps, and infrastructure to the cloud reap many benefits, but they must also give up some control over their data in the process. Users do not possess, operate, or control the computers that process the information. Because the user has no idea how the provider treats the data, a great deal of faith is required in this case. Significant adjustments to privacy and security protocols are necessitated by the inability to manage the system's physical and logical components. Even in terms of security, there is currently an absence of SLAs between service providers and their customers. Our studies focus on suitable security measures that may be able to satisfy the regulatory standards of conventional systems. The use of biometrics in security has been more apparent in recent years, after years of intensive study into the topic. Research and implementation prospects for cloud data security have expanded with the integration of biometric technologies with cloud computing. The privacy-sensitive character of biometric data necessitates that biometric templates be kept private even by cloud service providers. Because user information cannot be changed in the same manner as alphanumerical passwords, this need is more significant.

RELATED WORK

offloading computation without offloading oversight:

Among the most alluring areas of technology today is cloud computing, which is appealing in part because of how flexible and inexpensive it is. Though there has been a dramatic uptick in interest and activity surrounding cloud computing, the concept is plagued by long-standing fears that threaten to derail its progress and ultimately ruin its potential as an innovative approach to IT procurement. Described in this study are the issues and how they have affected adoption. We also detail how the integration of current research directions could address many of the issues that are preventing widespread use. To be more specific, we contend that cloud computing can offer benefits to business intelligence compared to the current isolated alternative, provided that research into trustworthy computing and computation-supporting encryption continues to progress.

Securing Data Access in the Cloud in a Scalable and Precise Manner:

In the new computing paradigm known as "the cloud," users have access to shared computer resources over the Internet. With all its potential, this paradigm shifts data security and access management into a whole new ballgame, especially when users entrust cloud servers—which aren't in the same trusted domain as data owners—with critical information. Current solutions often utilize cryptographic techniques, such as revealing data decryption keys to authorized users only, to protect sensitive user data from untrusted services. On the other hand, when it comes to fine-grained data access control, these solutions will eventually cause the data owner to incur a large computational burden for key distribution and data administration. As a result, they don't scale well. The challenge of access control's fine-grainedness, scalability, and data confidentiality all need to be addressed concurrently. This paper tackles this difficult open problem by doing two things: first, the data owner can assign most of the computation tasks for fine-grained data access control to untrusted cloud servers without revealing the data's contents; and second, access policies can be defined and enforced based on data attributes. To do this, we bring together proxy re-encryption, lazy re-encryption, and attribute-based encryption (ABE) in a novel way. Notable features of our suggested method include user secret key responsibility and secrecy of access privileges. Based on our thorough investigation, our suggested system is both extremely efficient and shown to be secure according to current security models.

Making sure that data stored in the cloud is secure:

Some have speculated that cloud computing will be the IT industry's next big thing. Instead of keeping IT services under strict physical, logical, and human constraints, as in conventional solutions, cloud computing relocates databases and application software to massive data centers, where data and service management might not be entirely reliable. But there are a lot of unanticipated security risks associated with this one-of-a-kind quality. As a long-standing component of service quality, cloud data storage security is the primary topic of this essay. In contrast to earlier efforts, our proposed distributed approach is both effective and versatile, and it has two distinguishing characteristics that will help guarantee the accuracy of users' data stored in the cloud. Our technique locates data errors and ensures storage accuracy by combining the homomorphic token with distributed verification of erasure-coded data. This allows us to identify which servers are acting maliciously. Data update, deletion, and add are only a few examples of the efficient and secure dynamic operations that the new method offers, going beyond what most previous efforts have done. Byzantine failure, malicious data modification assaults, and server collusion attacks are all shown to be ineffective against the suggested method, according to thorough performance and security analyses.

Data ProtectionAware Design for Cloud Services. A Record of the First Global Summit on Cloud Computing:

Concerns around privacy, network security, data protection, and information assurance have not been completely resolved with the Cloud because it is a novel concept. To save money, this article aims to start building data protection rules into clouds from the beginning, rather than adding security as an afterthought. We begin by outlining a new capability maturity model and thinking about cloud maturity from an enterprise-level viewpoint. We apply this approach to investigate business cloud privacy measures and identify potential areas for data protection control design as cloud exploitation develops further. We show how design patterns may be used to provide such controls. Lastly, we take into account the potential usage of Service Level Agreements (SLAs) to guarantee that third-party vendors support these regulations.

METHODOLOGY

We have utilized a biometric database including the photos of ten individuals to carry out this study. You can see these images on the screen below.

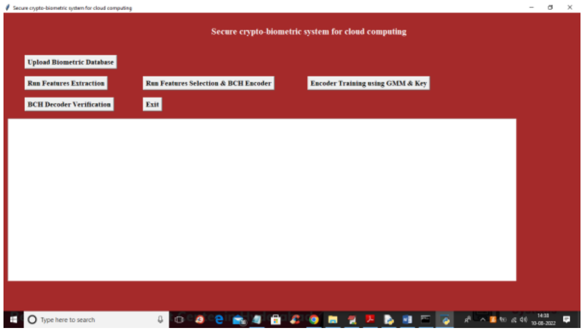
To implement this project we have designed following modules

1) Upload Biometric Database: This module will be used to submit a database of biometric templates to the application.
2) Run Features Extraction: Features may be extracted from templates with the help of this module.

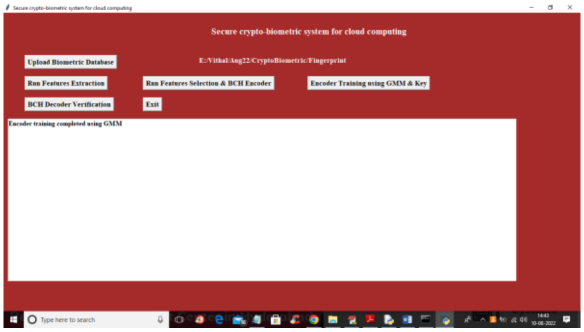
DOI: https://doi.org/10.61841/turcomat.v15i3.14776

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

RESULT AND DISCUSSION


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
Run Features Extraction
Run Features Selection & BCH Encoder
Encoder Training using GMM & Key
BCH Decoder Verification
Exit
Type here to search

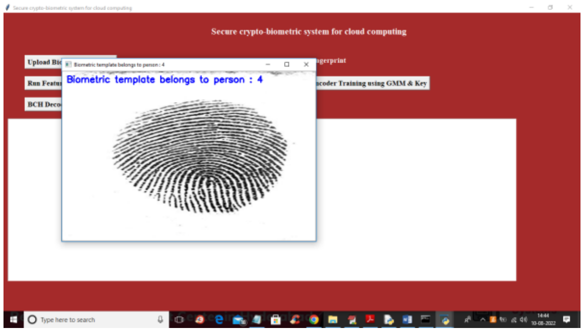
In above result click on 'Upload Biometric Database' button to upload database and get below screen


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
Run Features Extraction
Run Features Selection & BCH Encoder
Encoder Training using GMM & Key
BCH Decoder Verification
Exit
Type here to search

E:/Vithal/Aug22/CryptoBiometric/Fingerprint

```
Encoder training completed using GMM
```

In above result GMM training completed and now click on 'BCH Decoder Verification' button to upload TEST template and get below output


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Bio
Run Featu
BCH Deco
gerprint
coder Training using GMM & Key
Biometric template belongs to person : 4
Type here to search
14:44
10-08-2022

Biometric template belongs to person : 4

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

CONCLUSION

Critical data on the cloud is the focus of our suggested practical safe cryptographic technology. Access to the data is made accurate and safe by biometric identification. Our methodology assures that the cloud does not know either the user's biometric data or the outcome of the biometric private matching identification, which is a big distinction from other biometric schemas. Our methodology is built to be secure and compliant with the law since it does not use a direct matching procedure. Our suggested solution safeguards the user's biometric information while enabling the verifier to verify their identity. The security features offered by third-party cloud apps are well-suited to this architecture. To strengthen the schema's models and hence its security, a training mechanism has been suggested. To efficiently complete tasks that need a lot of processing power, our training system makes advantage of cloud resources. A traditional method of authentication using public and private keys is used. This paves the way for the system to leverage any and all certification authority-based infrastructures and solutions that may be available. Our cryptobiometric system has some room for improvement. One major drawback is how long it takes for a client app to process biometric data. Our schema-dependent apps' responsiveness and engagement might be negatively impacted if the processing time for user biometric data takes too long due to a complicated combination of models (a few seconds in the instance of a 16-UBM system, as mentioned earlier). Improving process time should be the subject of a comprehensive inquiry. Cloud computing resources may prove to be quite beneficial in this regard. Therefore, future research should focus on finding a secure method to handle biometric data that prevents it from being available to third parties, such as the cloud provider. At long last, a comprehensive SaaS solution It is possible to create a solution that offers our approach's capabilities as a service.

REFERENCES

[1] Balachandra Reddy Kandukuri, Ramakrishna Paturi V., Atanu Rakshit, Cloud Security Issues IEEE International Conference on Services Computing 2009, IEEE SCC 2009: 517-520, Bangalore, India, Sep 2009.

[2] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW ’09): 85-90, ACM, New York, Nov 2009.

[3] 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.

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

[5] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, Data ProtectionAware Design for Cloud Services. Proceedings of the 1st International Conference on Cloud Computing, CloudCom ’09, LNCS 5931/2009: 119- 130, Beijing, China, Dec 2009.

[6] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing, Computer Security ESORICS 2009, LNCS 5789, Springer: 355-370, Saint-Malo, France, Sep 2009.

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

[8] D. Kesavaraja, D. Sasireka, and D. Jeyabharathi, Cloud Software as a Service with Iris Authentication, Journal of Global Research in Computer Science, 1(2): 16-22 September 2010.

[9] S. Suryadevara, S. Kapoor, S. Dhatterwal, R. Naaz and A. Sharma, Tongue as a Biometric Visualizes New Prospects of Cloud Computing, 2011 International Conference on Information and Network Technology, IPCSIT 4(2011): 73-78, Chennai, India, Apr 2011.

[10] N.K. Ratha, J.H. Connell, and R. Bolle, Enhancing Security and Privacy of Biometric-Based Authentication Systems, IBM Systems Journal, 40(3): 614–634, 2001.

[11] 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.

[12] A. Goh, D.C.L. Ngo, Computation of Cryptographic Keys from Face Biometrics, 7th IFIP-TC6 TC11 International Conference, CMS 2003, Lecture Notes in Computer Science, 2828/2003: 1-13, Torino, Italy, Oct 2003.

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

[14] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, A. Neri, Cancelable 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.

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

[16] P. Kenny, G. Boulianne, P. Dumouchel, Eigenvoice Modeling With Sparse Training Data, IEEE Transactions on Speech and Audio Processing, 13(3): 345-354, 2005.

[17] C. Vielhauer, R. Steinmetz, Handwriting: Feature Correlation Analysis for Biometric Hashes, EURASIP Journal on Applied Signal Processing, 2004(4): 542-558, 2004.

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

[19] P. Tuyls, A. Akkermans, T. Kevenaar, G.J. Schrijen, 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.

[20] M. Van der Veen, T. Kevenaar, G.-J. Schrijen, T.H. Akkermans, and F. Zuo, Face biometrics with renewable templates, SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents, 6072: 205-216 San Jose, CA, USA, Jan 2006.

[21] F. Hao, R. Anderson, J. Daugman, Combining crypto with biometrics effectively, IEEE Transactions on Computers, 55(9): 1081-1088, 2006. [22] K. Simoens, P. Tuyls, B. Preneel, Privacy Weaknesses in Biometric Sketches, 30th IEEE Symposium on Security and Privacy: 188-203, Oackland, CA, USA, May 2009.

[23] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, B. Dorizzi, ´ Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris, Biometrics Symposium, 2008. BSYM’08: 59-64, Tampa, Florida, USA, 23-25 Sept. 2008.

[24] J.L. Alba-Castro, D. Gonzalez-Jim ´ enez, E. Argones-R ´ ua, E. Gonz ´ alez- ´ Agulla, E. Otero-Muras, Carmen Garc´ıa-Mateo, Pose-corrected face processing on video sequences for

webcam-based remote biometric authentication, Journal of Electronic Imaging, 17(1): 011004, 2008.

[25] E. Argones Rua, D. P ´ erez-Pinar L ´ opez, J.L. Alba-Castro, ´ Ergodic hmmubm system for on-line signature verification, Joint COST 2101 and 2102 International Conference, BioID MultiComm 2009, Lecture Notes in Computer Science, 5707/2009: 340-347, Madrid, Spain, Sep 2009.

[26] L. E. Baum, T. Petrie, G. Soules, N. Weiss, A Maximization Technique Occurring in the Statistical Analysis of Probabilistic Functions of Markov Chains, The Annals of Mathematical Statistics, 41(1): 164-171, 1970.