Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 3372 – 3378

An Extensive Study on Biometric based Secure Data Computing Framework for Mobile Cloud Environments

A.Amali Mary Bastina[1], Dr.N.Rama[2]

Department of computer Science[1], Department of computer Science[2]

Loyolo College, Chennai[1], Presidency College, Chennai[2]

Abstract

Mobile cloud computing is gaining popularity among mobile users as it is considered as long envisaged vision of computing as a utility. Despite of its popularity, innovative advances in hardware, networking, middleware, and virtual machine technologies have led to an exploration of new, globally distributed mobile cloud computing platforms. Mobile Cloud Computing provides computation and storage from anywhere around the world via the Internet without adopting for purchase of new infrastructure, training, or software licensing. Mobile cloud is a service model which has been used by mobile device for information storage, searching and data mining and multimedia processing. In addition, this advanced computing platform brings many new challenges for data security and access control on the user data stored on cloud servers. As the data users, no longer have physical possession of the outsourced data, makes the data integrity, privacy and authenticity protection in Cloud Computing a very challenging and potentially difficult task. In order to tackle those challenges, cryptography based secure architecture has been employed to effectively disseminate the user to access the data stored by the data owner. However those techniques further leads to heavy computational time and cost. In this paper, an extensive study has been carried out using biometric based authentication architecture to strengthen the security of data stored in the cloud environment. It is vital and essential task for providing detailed insight on those authentication systems. The efficacy of each model has been demonstrated on single modal and multimodal fusion. Moreover importance of fusion based representatives has been exploited for secure data access paradigm. Finally outline of the proposed methodology as framework to secure data access using biometric based system has been provided. Evaluation of models has been carried out on the processing of the biometric images of the data users.

Keywords: Mobile Cloud Computing, Security, Biometric Authentication, Multimodal Security, Feature Extraction, Face Recognition, Fingerprint Recognition

1. Introduction

Mobile Cloud Computing (MCC) is a concept which is a combination of mobile environment and cloud computing[1][2]. It provide many facilities and services in all fields, like computing and storage, internet based services etc. Basically MCC provide its user the ability to

access and manage the data and application at anytime, anywhere and that to at the low cost. However, significant attention remains focused on security concerns[3]. 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. While providing secure access to cloud services is not a trivial task, and designing robust authentication[4], authorization[5] and accounting for access is an ongoing challenge, both operationally and research-wise.

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. Biometric images like face and fingerprint has been used for authentication based on the feature selection and classification model. The user requests the data access by sending the face image or Fingerprint captured through mobile device[6]. Acquired image undergoes feature selection and classification towards authentication and verification of the user towards data access in the cloud environment.

Biometric possesses a lot of advantages like portability, uniqueness and verification from unauthorized access by malicious users. However an extensive study on the biometric based secure data access architecture in the mobile cloud environment will help us to model a secure data access framework based on fusion of multimodal biometric data[7]. Fusion based multimodal biometric authentication systems are developed to explore an effective way to secure data access on information of data owner. The remainder of this paper is organized as follows: We discuss the review of literature in Section 2 and presents deep learning technique for trajectory mining models in Section 3. Section 4 provides objective of the work and section 5 outlines the proposed methodology. Section 5 provides conclusion of the work.

2. Review of Literatures

In this section, various existing model applied to authentication of outsourced data in the cloud environment using fusion various biometric using machine learning algorithm for process of classification and verification which has been detailed as follows.

2.1. Center-Less Single Sign-On With Privacy-Preserving Remote Biometric-Based ID-MAKA Scheme for Mobile Cloud Computing Services

In this method, Identity-based mutual authentication between a mobile user and data stored in mobile cloud environment has been analysed. Mobile cloud computing paradigm is to make authentication for data access with more usability, security and scalability. Remote biometric-based authentication has been considered with single sign-on and center-less authentication. The model has been analysed as design principle for secure data access. Therefore, the user can access multiple clouds computing outsourced data by registering biometric images in the registration center, and cloud computing servers can complete the biometric-based remote authentication and verification for the user on the participating list[8]. In this way, the scheme greatly improves usability, scalability, and security as effective solutions to provide a formal security proof by using Real-Or-

Random(RoR) model and Burrows-Abadi-Needham (BAN) logic to show that the scheme is secure and security analysis for other known attacks.

Drawbacks of the model

- Verification of the user on specified biometric will produce large no of features for classification, hence it leads to large computational cost and time.
- System in ineffective against man in middle attack.

2.2. Secure Finger print based biometric system for cloud computing

In this method, Crypto biometric system has been enabled to heterogeneous group of providers and Mobile cloud-based services. Initially pre-processing as reshapping is employed to acquire image. This reshaping destroys the spatial information/relation and dependent structure of the variables to their local neighbourhoods. The model uses the feature extraction using hidden markov model to extract region of interest. The extracted biometric information is then protected by means of error-correcting codes. Pattern matching model is employed on the extracted features trough KNN classifier model[9]. Further pattern matching generates the match score amongst the image captured and the image in the cloud database.

Drawbacks of the model

- Redundant information present in the biometric will lead to high false acceptance rate.
- Due to sparsity of the data, it leads to over fitting problem.

2.3. Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services

A number of the security frameworks presented in the survey deal with the security of files/data created and manipulated on a mobile device or cloud servers In this method, a unique identity from the user's biometric data has been employed for authentication which is further used to generate the verification process for data access stored in the cloud. In addition, we propose an efficient approach to generate a verification process through machine learning model for identifying the user between two communicating parties using two biometric templates for a secure message transmission[10]. In other words, there is no need to store the index data for the user biometric information anywhere.

Drawbacks of the model

- Template Matching is easily indistinguishable on large scale of biometric image which further reduces accuracy of the recognition
- Template matching explored only with least explored data will be degrade the performance accuracy.

2.4. Hash based Blowfish User Authentication through Biometric data for Secure Data Access

In this method, preserving data from unauthorized users is carried out using biometric authentication. Further to improve authentication accuracy, hash based blowfish authentication is

introduced for accessing data from server on the provided biometric. It comprises three steps, namely Registration, Authentication and Ticket Granting. In the Registration process, client provides user details in terms of biometric image and those data is stored on cloud server (CS) using hashing function. When user wants to access data of the data owner in the server, authentication server (AS) verifies user identity by sending a message. When authenticity is verified, AS accepts user as authenticated user and convinces CS that user is authentic. For convincing process, AS generates a data using Blowfish mechanism[11]. Finally, the server provides the data using blowfish verification.

Drawback of the model

- Hash Based Blow fish model limited to single biometric
- Discovering the comorbidity relationship is very hard**.**

2.5. Data Security Enhancement in Cloud Computing Using Multimodel Biometric System

In this method, a new multimodal biometric system that is possible for the future smartphones to be supported where one can upload, download or modify the files using cloud without worrying about the unauthorized access of any third person as this security authentication uses combination of multiple security system available for verification of the user towards data access. Further it effective against various kinds of attacks and it support the data dynamics on storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication through explore of the technique of bilinear aggregate signature and usage of maximum entropy expectation maximization algorithm[12].

Drawbacks of the model

- Complexity in determining extract user match for each block of data.
- It is unable to estimate the block on slight changes in the data.

3. Overview of Biometric based Secure Data computing architecture

Biometric based secure data computing architecture necessitates the modelling of data access and verification which inherently have spatial and temporal dependencies. Data owner uploads file and information to the cloud to enjoy various benefits, stored information of the data owner are episodic and irregular in time[13]. Biometric authentication model learns the features of the biometric traits and infers similarity of the features on distance measures to provide authentication to data access. Multimodal Biometric Authentication is to handle irregularly timed events by moderating the spatial and temporal information through image transformation and consolidation of the transformed images is explicitly captures the change of the feature orientation effectively. Finally Confounding interactions between data user and data owner has been determined. Multimodal biometric learning is capable of handling complexity in data in terms of variable length and data dependencies.

4. Objective of the work

Research was focused on securing data access in the mobile cloud environment based on multimodal biometric authentication technique. The objective of this study is to acquire and verify the data user on feature fusion and feature selection using multimodal biometric images. The prediction technique towards identification of the user towards data access and access response to the data has been computed on the stored biometric data. The objective of the work is on biometric data can be constructed using Expected maximization algorithms to predict the user towards data access of user stored in the cloud[14]. Further feature selection on following aspects is carried out to determine the regions related to the volumetric change and orientation changes of the image.

5. Outline of the methodology

In Secure data access paradigms, analysing of the large amount of data with sequence of verification model using biometric authentication provide more accuracy and it ease to determine the user on more significant characteristics of extracted biometric of the user is becoming essential in current research. To enable the effective solution, a novel framework has to be established on inclusive of solutions to handle above mentioned difficulties. The framework composed of methodology is as follows

5.1. Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access

In this model, finger biometric authentication model has been used to secure the data access in the cloud environment. On each biometric acquired data, the secret code is generated by entropy value[15]. The generated value will be enabled on the person to request for accessing the data in the mobile cloud server. During data user, requesting the data access to stored data, the authorization of the user will undergoes computation. Result of verification, system sends the permit access and user can be access the data.

5.2. Authentication for data access with face recognition system on mobile cloud environment

In this model, Face recognition is used for user Authentication using mobile devices for accessing the data from the cloud. In this methodology, face biometric authentication model works as recognition model on extracting the knowledge from Discrete cosine transform and and Extreme learning machine (ELM). These architecture is proposed in mobile cloud computing. Towards request for data access, user requests by sending the face image captured through mobile via Bluetooth to the computing model[16]. The DCT coefficient is applied over the captured image to acquire the values to compare the values of image which is already stored in cloud storage. The image values are compared by using the ELM distance classifier. If the values are matched, then the data owner grants permission to that user if not the request is denied. Once approval is given by data owner, user can access the particular data in the cloud.

5.3.Secure Data Access Computing Model on Mobile Cloud Data using Fusion of Finger Print and Face biometric authentication based on Discrete Combinational models

In this model, multimodal biometric based authentication technique has been employed as a fusion model on finger print and face patterns. Initially feature selection methods explore intrinsic finger print and face features using principle component analysis and linear discriminant analysis in selecting high relevant features. Feature fusion carried out on outcomes of PCA and LDA technique using discriminant correlation analysis. The proposed system uses differential model to determine the less no of optimal features for multimodal authentication.

6. Importance of Multimodal Fusion based Secure Data computing framework

Advanced cloud-assisted mobile multimedia services have been exploited by the owner to share their multimedia data via the cloud platform to enjoy the flexibility[17]. However, the several challenges of the environment has raised importance of data security and privacy concerns while enjoying the rich computation and storage resources towards saving the overhead of mobile devices. In particularly, enforcing the access control to outsourced data to the cloud has vital and the data owner has to rely on the cloud server and cloud server cannot be fully trusted[18]. A well adoptable approach is to encrypt the multimedia data before offloading it to the cloud**;** however it might lead to complicated key distribution and management.

Multimodal based Biometric authentication is easy to be acquired and difficult to be forged. Further it enhances the recognition rate on fusion of fingerprint and face based authentication system using various machine learning processes[19]. Combinational model generate optimal subset of features using differential evolution. Finally it produces better results less computational cost and time. It is superior in computing comorbidity relationships and features are easily distinguishable on large scale data. It is secure against various types of attacks[20].

Conclusion

In this paper, an extensive study on the Biometric authentication technique to secure data access in the mobile cloud environment has been presented in detail. It has been analysed on various biometric features employed for the proposed architecture from different literatures on basis of extracting the time varying features and clustering it based on similarities. Especially prediction model deals on progression accurately on the underlying features. These analyses help to model a new methodology as framework for authentication and verification of the user.

References

[1] F. Liu, Y. Yin, G. Yang, L. Dong, and X. Xi, “Finger print recognition with superpixel-based features,” in Proc. Int. Joint Conf. Biometrics (IJCB), Florida, USA, Sep./Oct. 2014, pp. 1–8

[2] J. Yang, Y. Shi, and G. Jia, “Face Image Matching Based on Adaptive Curve Transformation,” Pattern Recogn., 2017.

[3] B. A. Rosdi, C. W. Shing, and S. A. Suandi, “Finger vein recognition using local line binary pattern,” Sensors, vol. 11, no. 12, pp. 11357– 11371, 2011.

[4] J.-D. Wu and C.-T. Liu, “Finger-vein pattern identification using principal component analysis and the neural network technique,” Expert Syst. Appl., vol. 38, no. 5, pp. 5423–5427, 2011.

[5]. Fan Z,Xu Y,Zhang D. Local linear discriminant analysis framework using sample neighbors. IEEE Transactions on Neural Networks, 2011, 22(7):1119-1132
[6]. Kumar, K. V & Negi, A "Novel approaches to principal component analysis of image data based on feature partitioning framework" in Pattern Recognition Letters, 29, 254–264, 2008
[7]. Shazeeda and Bakhtiar Affendi Rosdi "Finger Vein Identification based on the Fusion of Nearest Neighbor and Sparse Representation based Classifiers" Indian Journal of Science and Technology, Vol 9, 2016
[8]. Wenzheng Liu, Xiaofeng Wang, Wei Peng , Qianqian Xing"Center-Less Single Sign-On With Privacy-Preserving Remote Biometric-Based ID-MAKA Scheme for Mobile Cloud Computing Services" In IEEE Access, Vol.7, 2019
[9]. Gaurangkumar Panchal, Debasis Samanta, Ashok Kumar Das, Neeraj Kumar"Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services" in IEEE Transactions on Cloud Computing, 2020
[10]. Sunil Kumar Khatri, Monica, Vikas Rao Vadi"Biometrie based authentication and access control techniques to secure mobile cloud computing"in International Conference on Telecommunication and Networks, 2017
[11]. K. Mohana Prabha & P. Vidhya Saraswathi"Hash based Blowfish User Authentication through Biometric data for Secure Data Access" in International Conference on I-SMAC,2018
[12] Kuhu Singh,Anil Kumar Sajnani,Sunil Kumar Khatri "Data Security Enhancement in Cloud Computing Using Multimodel Biometric System" in International conference on Electronics, Communication and Aerospace Technology 2019.
[13] J. Chai, H. Liu, B. Chen, and Z. Bao, “Large margin nearest local mean classifier,” Signal Processing, vol. 90, no. 1, pp. 236-248, Jan. 2010.
[14] A. M. Martinez and A. C. Kak, “PCA versus LDA,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 23, no. 2, pp. 228– 233, 2001
[15] A. Amali Mary Bastina & N. Rama "Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access" in International Journal of Electrical and Computer Engineering (IJECE), vol.7,2017
[16] A. Amali Mary Bastina & N. Rama "AUTHENTICATION FOR DATA ACCESS WITH FACE RECOGNITION SYSTEM USING MOBILE CLOUD COMPUTING" in journal of advanced research in dynamical and conrol system.
[17] G. Yang, X. Xi, Y. Yin, ”Finger vein recognition based on (2D)2 PCA and metric learning,” BioMed Research International, vol. 2012, no. 2012, pp. 324249-324258, May.2012.
[18] H. Qin, L. Qin, C. Yu, ”Region growth-based feature extraction method for finger-vein recognition,” Optical Engineering, vol. 50, no. 5, pp. 057208-057208, May.2011
[19] N. Miura, A. Nagasaka, T. Miyatake, ”Extraction of finger-vein patterns using maximum curvature points in image profiles,” IEEE transaction on Information and Systems, vol. 90, no. 8, pp. 1185-1194, Aug.2007.
[20] H. C. Lee, B. J. Kang, E. C. Lee and K. R Park,”Finger vein recognition using weighted local binary pattern code based on a support vector machine,” Journal of Zhejiang University SCIENCE C, vol. 11, no. 7. pp. 514-524, Jul. 2010.