Multimodal Biometric Authentication using Gray Level Co-Occurrence Matrix for Enhancing Security in Cloud

1M. Shyamala Devi, 2B. Mahalakshmi and 3P. Balamurugan

1Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai.
shyamalapmr@gmail.com

2Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai.
jeevamaha.lakshmi@gmail.com

3Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai.
pookumbala@gmail.com

Abstract

Clouds are flattering to be widespread service providers due to their low upfront costs, rapid application deployment, and high scalability. Numerous users outsource their sensitive data and services to cloud service providers. Users repeatedly access their sensitive data services through devices and connections that are vulnerable to thieving and eavesdropping. As a result, the users are fraught of robust security measures to protect their sensitive data and service privacy in clouds. Multimodal biometrics is an emerging research area to investigate for enhancing the security of cloud. It is used for recognize the individuals for providing security in the application and also to increase the security levels. In General, the highly secured systems are generally accessed to be computationally expensive systems. The concept of Perception Learning Rule is applied for implementing the authentication process in the biometric system which provides more security. Here we try to provide a survey of biometric authentication system that is used to provide the security in cloud. We also designed Multimodal Biometric Systems by Gray level Co-occurrence matrix which enhances the feature extraction.

Key Words: Authentication, multimodal biometric, outsource, security.
1. Introduction

Cloud Computing is emerged in the world of computer science in order to change and improve the methodology that are used to outsource the Information Technology services. Still it has drawback related to the security risk issues. Though it uses the methodology like passwords (knowledge-based security) and ID-cards (token-based security), still it has some security issues. However, security can be easily breached in these applications when a password is released to an unauthorized user. It is also possible for the unauthorized users to process Keyword Guessing Attack. The emergence of biometrics has addressed the problems that weaken traditional verification systems. Generally the Biometrics refers to the automatic identification of an individual by using some physiological or behavioural qualities associated with the person. Authentication is the process of identifying an individual using security system and it is an essential one that is to be carried out in any application. Traditional techniques for user authentication could be categorized as [1, 2]:

1. Token based techniques (i.e. key cards and smart cards)
2. Knowledge-based techniques include text-based and picture-based passwords (mixture of username and password).

However the above two methods are vulnerable to attacks. It could be easily lost or forgotten. Generally the traditional techniques are considered to be not reliable or secure, and are not presently sufficient in some security application zones. The primary advantage of biometrics is that it cannot be misplaced, forgotten or stolen. Due to greater accuracy and higher robustness of biometric recognition [1], the biometric solutions have become popular and preferred methods to analyze human characteristics for security, authentication and identification purposes. It could not be duplicated or counterfeited and misused. Practically, the use of biometrics information is the most secure method. Consequently, it is now needed in many fields such as surveillance systems, security systems, and physical buildings. Other applications of biometrics systems include: access control (access to computer networks), forensic investigations, verification and authentication, e-commerce, online banking, border control, parenthood determination, medical records management, welfare disbursement and security monitoring. In the most general definition, "Biometric technologies" is defined as an automated methods of verifying and recognizing the identity of a living individual based on two categories: (1) Physiological biometrics include (Facial, hand and hand vein infrared thermogram, Odor, Ear, Hand and finger geometry, Fingerprint, Face, Retina, Iris, Palm print, Voice, and DNA), and (2) Behavioral biometrics like (Gait, Keystroke, Signature) which measure the human actions [8]. Also, human electrocardiogram (ECG) signal is considered one of Biometric features used in individual recognition and authentication [11]. The usage of Multimodal Biometric System focuses to improve the effectiveness of security and reliability of the application by reducing the following parameters.

- **FAR**: False Accept Rate
2. Related Work

Wenmin Li [5] states that Classification based on Multiple Association Rules. The method extends an efficient frequent pattern mining method, FP – growth, constructs a class distribution-associated FP-tree, and mines large database efficiently. Reza Fathi [3] states that at each level, the architecture focus on authentication factors by considering the perceived hardship for users. To increase the security and user convenience, the architecture also considers the implicit authentication factors in addition to the explicit factors. Jun Zhou [9] states that Fusion of face and finger print by support vector machine (SVM) which introduced a new normalization method improved the authentication accuracy. A new concept of optimal two-dimensional face is proposed to improve the performance of the dynamic face authentication system. E. Sasi [4] states that the electronic key to enter into the cloud by the user. The electronic key is given by the admin. For viewing the data biometric authentication is used. K. Sasidhar [8] states that Multimodal biometric systems perform better than uni modal biometric systems and are popular even more complex also. They examine the accuracy and performance of multimodal biometric authentication systems using state of the art Commercial Off-the-Shelf (COTS) products. Abdeljebar Mansour[2] states that to integrate a Class-Association Rules (CARs) into the process of Multi-factor Authentication Based on Multimodal Biometrics (MFA-MB) for Cloud Computing. It defines a new metric to measure the User Experience and, it exhibits an algorithm to authenticate cloud SaaS/PaaS Users with an enhanced MFA-MB scheme. Abdeljebar Mansour [1] states that Multimodal biometrics can be considered as an alternative solution and additional factor to increase CC authentication security level. Jonas Richardi [6] states that how information can be used in a uni modal and multimodal context, and we perform objective evaluation of quality measures on multimodal benchmarking databases.

3. Existing Techniques

3.1. Classification based on Multiple Association Rules

Wenmin Li [5] proposed that associative classification has high classification accuracy and strong flexibility at handling unstructured data. However, it still
suffers from the huge set of mined rules and sometimes biased classification or overfitting since the classification is based on only single high-confidence rule. In this study, we propose a new associative classification method, CMAR, i.e., Classification based on Multiple Association Rules. The method extends an efficient frequent pattern mining method, FP-growth, constructs a class distribution-associated FP-tree, and mines large database efficiently. Moreover it applies a CR-tree structure to store and retrieve mined association rules efficiently, and prunes rules effectively based on confidence, correlation and database coverage. The classification is performed based on a weighted \( x^2 \) analysis using multiple strong association rules. Their extensive experiments on 26 databases from UCI machine learning database repository shows that CMAR is consistent, highly effective at classification of various kinds of databases and has better classification accuracy in comparison with CBA and C4.5.

### 3.2. User Friendly Authentication

Reza Fathi[3] states that robust authentication techniques are demanded by users for safe access to cloud services. They propose a technique which uses multiple authentication factors to access cloud services. But the major challenge is that the multi-factor authentication technique is not effective as it causes user frustration and fatigue. To address this challenge, they propose a multi-factor authentication architecture that mainly focuses on minimizing the perceived authentication hardship for cloud users thereby improving the authentication security. To achieve this, their authentication architecture suggests a progressive manner to influence access to diverse levels of cloud services.

At each level, the architecture asks for authentication factors by considering the perceived hardship for users. To increase the security and user convenience, the architecture also considers implicit authentication factors in addition to the explicit factors. Their evaluation results indicate that authentication using the proposed architecture decreases the users’ perceived hardship up to 29% in compare with other methods. The results also reveal that our proposed architecture adapts the authentication difficulty based on the user condition.

### 3.3. Support Vector Machine (SVM) Authentication

JunZhou[7] proposed This paper presents a novel face and fingerprint identity authentication system based on multi-route detection. To exclude the influence of pose on face recognition, a multi-route detection module is adopted, with parallel processing technology to speed the authentication process. Parallel processing technology is used to speed the authentication process. Fusion of face and fingerprint by support vector machine (SVM) which introduced a new normalization method improved the authentication accuracy.

A new concept of optimal two dimensional face is proposed to improve the performance of the dynamic face authentication system. Experiments on a real database showed that the proposed system achieved better results compared with face-only or fingerprint-only system.
3.4. Electronic Key Authentication

E. Sasi [4] focuses on Internet authentication, where people often discuss about passwords. One of the main problems with current authentication approaches is the existence of too many password account pairings for each user, which leads to forgetting or using the same username and password for multiple sites. They address this problem by using the concepts of biometrics.

Biometric authentication techniques try to validate the identity of an user based on his/her physiological or behavioral traits. Comparable issues are also encountered in other operation domains of biometric technology, such as forensics and law-enforcement. Cloud security is provided by biometric techniques such as Iris authentication and fingerprint. They use a new method as Electronic key which is generated uniquely for an individual user. It is the combination of the data’s like encoded information and the ID of the user. Electronic Key is verified at each time in authentication. Finger Print and Iris verification is highly increase efficiency of authentication.

3.5. Multimodal Biometric Authentication Systems

K.Sasidhar [8] discusses the concepts of Multimodal biometric systems which are providing identification and human security over last few decades. Some of these multimodal systems are human computer dialog interaction based systems where the user interacts with the PC through voice or vision or any other pointing device in order to complete a specific task. Multimodal biometric systems are those which utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. A biometric system measures and analyzes human body physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes or behavioral characteristics. However unimodal biometric solutions also have limitations in terms of accuracy, enrolment rates, and susceptibility to spoofing. This limitation occurs in several application domains, example is face recognition. The accuracy of face recognition is affected by illumination and facial expressions. The biometric system cannot eliminate spoof attacks. A recent report by the National Institute of Standards and Technology (NIST) to US concluded that approximately two percent of the population does not have a legible fingerprint. By considering all the above factors, they propose a new approach to the multimodal biometric system. This new Multimodal biometric systems perform better than unimodal biometric systems. They examine the accuracy and performance of multimodal biometric authentication systems using state of the art Commercial Off- The-Shelf (COTS) products.

3.6. Multi Factor Authentication based on Multimodal Biometrics

Abdeljebar Mansour[2] confer that cloud consumers store their personal or sensitive business data in cloud service providers which are located in different geographical areas of the world. So, these data should be protected from being accessed by unauthorized persons. So the cloud service
providers need to develop a secure and efficient authentication methods aiming to overcome the security issues mainly related to data leakage and security attacks. So they proposed a new approach to implement multimodal biometric systems for authentication and identity management using user’s physiological and/or behavioral traits. Second, combining the advantages of multi-factor and multimodal biometric techniques they also develop a hybrid scheme called Multi-factor Authentication based on Multimodal Biometrics (MFA-MB) in order to authenticate for cloud consumers.

3.7. Class-Association Rules for Authentication

Abdeljebar Mansour [1] states that highly secured systems may also corrupt the user experience. They develop a system with three modules. The first module integrates a Class-Association Rules (CARs) with the process of Multifactor Authentication Based on Multimodal Biometrics (MFAMB). The Second module defines a new metric to measure the User Experience. The third module demonstrates an algorithm to authenticate cloud SaaS/PaaS Users with an enhanced MFA-MB scheme. Since, CARs are used to predict the most expected Multimodal Biometric Authentication in the source of Users’ authentication habits, mined from their historical authentication data sets, which guarantees continuously improving their Experience. They show that their system increases the authentication security level using MBA at a decreased time and improved user experience.

3.8. Multi Model Biometric Verification

Jonas Richiard[6] review the various approaches that have been used to extract additional information about the biometric data that can be used to improve performance in degraded conditions. They also present a system that does not depend on specific modalities, including new user-model based quality measure. They show how this information can be used in a unimodal and multimodal context. They also perform objective evaluation of quality measures on multimodal benchmarking databases.

4. Drawback of the Existing Techniques

4.1. Classification based on Multiple Association Rules

- Classification based on Predictive Association Rules low
- Lower running time

4.2. User Friendly Authentication

- secret splitting
- some random sequence checking
- Password guessing attack

4.3. Support Vector Machine (SVM) Authentication

- In effective min- max normalization

4.4. Electronic Key Authentication

- Special equipment must be present when the identifiers are issued or verified.
- Usage of special equipment would add increase the maintenance cost
• The biometric identifier should be digitized for administrative purpose.
• Digitized images would require large amounts of storage.

4.5. Multimodal Biometric Authentication Systems
• Low False Acceptance Ratio
• The accuracy of the system get reduced

4.6. Multi Factor Authentication based on Multimodal Biometrics
• Less Security
• Reduce Speed
• Low Matching Score

4.7. Class-Association Rules for authentication
• Reduce speed
• Too many parameters are used in class association rule

4.8. Multi Model Biometric Verification
• Accuracy does not depend too much on confidence and coverage threshold

5. Proposed System

5.1. Multi Modal Biometric Authentication with GLCM

Multimodal Biometric Systems is implemented in the proposed system. In the multimode biometric system Multimodal Biometric Systems (MBSs), as indicated by their name, use a multiple source of information for authentication. MBSs are able to meet the stringent performance requirements imposed by various applications. In multi biometric system In Fusion at the Matching Score Level, each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as ‘weighted averaging’ may be used to combine the matching scores reported by them multiple matchers. An algorithm to authenticate cloud SaaS/PaaS Users with this new scheme and provide a solution to control/keep a low complexity while increasing the security level.

5.2. Gray Level Co-Occurrence Matrix

Gray Level Co-Occurrence Matrix(GLCM) has proved to be a popular statistical methods of extracting texture feature from images. According to co-occurrence matrix, Haralick defines to extract the characteristics of texture statistics of remote sensing images. In this paper four important features, Angular second moment (energy), (inertia moment), Correlation, Entropy, and the inverse Difference Moment are selected for implementation. The GLCM functions characterize the texture of an image by calculating how often pairs of pixel with specific values and in a specified spatial relationship occur in an image, creating a GLCM, and then extracting statistical measures from this matrix. (The texture filter functions, described in Texture Analysis cannot provide information about shape, that is, the spatial relationships of pixels in an image.)
The basic GLCM algorithm is as follow:

1. Count all pairs of pixels in which the first pixel has a value i, and its matching pair displaced from the first pixel by d has a value of j.

2. This count is entered in the ith row and jth column of the matrix $P_{d[i,j]}$.

3. Note that $P_{d[i,j]}$ is not symmetric, since the number of pairs of pixels having gray levels $[i,j]$ does not necessarily equal the number of pixel pairs having gray levels $[j,i]$.

4. The elements of $P_{d[i,j]}$ can be normalized by dividing each entry by the total number of pixel pairs.

6. **Implementation Results**

We have implemented the Multimodal biometric Authentication system using GLCM with Java and the results are shown below.
Figure 2: Filter Parameters for FACE

Figure 3: Feature Extraction for FACE
Figure 4: Filter Parameters for EYE.

Figure 5: Feature Extraction for EYE.
This paper summarizes various Multimodal biometric Authentication techniques to enhance the security level in Cloud system. We have done a Systematic study on the Multimodal biometric authentication for cloud

7. Conclusion

This paper summarizes various Multimodal biometric Authentication techniques to enhance the security level in Cloud system. We have done a Systematic study on the Multimodal biometric authentication for cloud
empowered system. We have identified the techniques to enhance the user experience for authentication which enhances the security in cloud. The limitations of all authentication techniques are discussed. By the above survey, security challenge can be adopted with multimodal biometric authentication. We believe that this proposed system will make the researchers to shape their problem in the area of security in cloud system.

References


[5] Wenmin Li, Jiawei Han Jian Pei, "CMAR: Accurate and Efficient Classification Based on Multiple Class-Association Rules" IEEE International conference of Data Mining, 2001, pp. 369-376.


