Credit Card Endorsement using Biometrics in Cloud Computing


Computer Science Department, Anna University
E-mail : rathigopalakrishnan@gmail.com, meenakshi.arl@gmail.com, saranyachandran92@gmail.com, sindhuja012@gmail.com

Abstract – The project entitled “Credit Card Endorsement Using Biometrics in Cloud Computing” is based on the security issues related to data access and data storage in cloud computing. The application focused is on the credit card authentication. The concept of biometrics is integrated along with the cloud for secure data access. The existing system of the credit card allows the user to do the transaction but there is no security measure to verify whether the user is authenticated or not. It has many security threats. The proposed model overcomes these security threats by using fingerprint biometrics along with the cloud which enhances the security measures. Fingerprint biometrics is one of the popular and effective approaches for prior authorizing the users and protecting the information. The proposed method uses the fingerprint of the card holder that is given prior to the transaction to verify the authentication. The fingerprint is unique which enhances the security issues of the credit card and prevents forgery.

Keywords – Credit card, fingerprint biometrics, cloud, STFT algorithm, authentication, security.

I. INTRODUCTION

We are using many cards in our day to day life like credit card, petrol card, etc because of its ease of use. These cards are used in public places and hence it is exposed to many hidden risks behind it. The existing system in credit card usage over shops is very simple. When using the card, it only requires the card holder signature for verification, on the statement generated by the credit card terminal. This signature is verified only on a frequent time basis, (i.e.) only when the vendor produces these statements in the bank. This signature can easily be forged or copied by anyone. This requires a major change for user authentication, in the existing system. The proposed system uses biometrics for user endorsement. This includes the scenario of requiring the user’s fingerprint when using the card in shop. With the fingerprint retrieved the user identification is validated by matching it with the one stored in cloud along with card holder’s account details. Fingerprints are used because they are generally unique for all. It provides more security to the user. The proposed method uses cloud database for storing the details and the fingerprint of the card holder.

Consciously or unconsciously many cards are used in our day – to – day life. Among them credit cards are important and are for ready convenience they confer on the user. Using a credit card, especially remotely, introduces an element of risk as the card details may fall into the wrong hands resulting in fraudulent purchases on the card. Fraudulent or unauthorized charges may take months to dispute, investigate and resolve. When a credit card is lost or stolen, it remains usable until the holder notifies the issuer that the card is lost. The only common security measure on all the cards is a signature panel, but signatures are relatively easy to forge. The proposed method is based on the security of the credit card by using fingerprint biometrics. Biometric identification in credit card helps in verification through recognition of patterns without having to remember any passwords or PIN numbers. A credit card that incorporates fingerprint authentication system provides enhanced security as the loss of the card does not by itself puts one’s money at risk. Fingerprints offer tremendous invariability, changing only in size with age as they are highly resistant to modifications or injury. In terms of implementation too, the technology is superior. Next generation scanners can easily analyze below the surface of the skin, and can add pore pattern recognition in addition to the more obvious minutiae of fingerprint. Moreover, the fingerprint sampling unit is compact, rugged and inexpensive.

II. BIOMETRICS

Biometrics refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. It offers new perspectives in high- security applications while supporting natural, user-friendly and
Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. The term “Biometrics” has come to be associated with the automatic identification of a person based on a feature or characteristic. These may be based on either:

- A physiological characteristic such as a fingerprint or face.
- A behavioral characteristic such as a signature or voice.

A variety of methods and techniques are available today, with the most common being Iris/ Retina, Fingerprint, Voice, Signature, Face. Generally, face, signature and voice are considered to be a lower level of security than fingerprint and iris. The facial recognition is a cheap technology it has many disadvantages and the 2D recognition is affected by changes in lightning, the person’s hair, the age and their accessories. It requires camera equipment for user identification, thus, it is less likely to become popular until most PCs include camera as standard equipment. The voice recognition has less verification time and is cheap but the person’s voice can be easily recorded and can be used for unauthorized use. Its accuracy rate is low and an illness such as cold makes it difficult to identify the voice of the person. The signature recognition has less verification time but it can easily be copied and the individuals who do not sign in a consistent manner may have difficulty in enrolling and verifying. The retinal scanning is highly accurate but it has the stigma of consumer’s thinking it is potentially harmful to the eye and it is very expensive.

Among all the biometric indicators, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. Fingerprint recognition has emerged as one of the most reliable means of biometric authentication due to its universality, distinctiveness, permanence, and accuracy [2]. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutia points, the five basic fingerprint patterns are: arch, tented arch, left loop, right loop and whorl. Minutia points include ridge endings, ridge bifurcations, dots, islands, ponds, bridges, crossovers etc... Loops make up 60% of all the fingerprints, wholes make 30% and arches 10%. Fingerprints are generally considered to be unique, with no two fingers having the exact same dermal ridge characteristics.

Cloud computing is internet based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. In cloud computing communications, information security entails the protection of information elements, only authorized users are allowed to access the available contents [2]. Authentication of a person is required to access places of high security and can be done in several ways, verification by knowledge such as passwords, verification by possession such as ID cards or passports or verification by biometrics such as fingerprints [3]. A cloud computing environment has several key features. It is massively scalable, and can be encapsulated as an abstract entity that delivers different levels of services to customers outside the world. It is driven by economies of scale and the services can be dynamically configured and delivered on demand. The resource of the cloud can be anything IT related. In general, cloud provides application, computation power, storage, bandwidth, database etc. As the resource pool is very large, user can increase the application on cloud to any scale. It is fully under user’s control.

As cloud computing has these features, the security plays a major issue in the cloud. The security can be enhanced by the use of biometrics like finger print to enhance authentication. Due to steady increase in computing power and the advent of obtrusive, ease-to-use fingerprint sensors, fingerprints are used more frequently as a biometric identification and recognition. Since fingerprints are unique, even between identical twins they are perfect for various security uses. Consciously or unconsciously many cards are used in day-to-day life. Among them credit card is important. Thus for many applications like credit card and other password related issues, fingerprint biometrics can be used to provide secure transaction of data.

Cloud’s combination of low cost and high scalability, effectively unlimited processing power and storage, unprecedented agility and speed to market all support the qualities that the bank will need to complete and win in the future. All banks stand to gain significant benefits from cloud computing adoption, including new levels of strategic optionality. Banks can use cloud computing to enter and scale up in emerging markets more quickly at lower cost and less risk. One type of cloud is the private cloud which is built by applying virtualization within a bank’s own data centers. Because the private clouds are not exposed to external “tenants”, banks tend to regard them as a more secure environment for customer data. The cloud database used in the proposed method is Xeround cloud database. It provides a cloud database service for applications based on the
MySQL database. Xeround is a simple, powerful cloud database and an elastic, always-on database-as-a-service for the MySQL applications. It is a service that replaces the existing MySQL database and provides seamless MySQL scalability and high availability. Xeround runs in cloud, that allows automatic scaling of database and maintains availability even in the event of failure.

IV. PROCESS FLOW

The initial process is the bank gets the fingerprint of the card holder to update and store in their cloud database along with the credit card account information, where this fingerprint image is used for matching with the original fingerprint of the card holder during the credit card usage. The feature of the fingerprint is directly stored in the database. The proposed method as shown in Fig. 1. integrates the fingerprint scanner and the credit card machine with the system of the vendor where the software is hosted. The credit card is swiped in the credit card machine and the card number is sent as input whereby the fingerprint scanner scans the fingerprint of the card holder and the image is sent as input to the system of the vendor. With the given number as input it is sent to the cloud database of the bank via the bank server, where the respected fingerprint image of the holder is retrieved and it is sent back to the server. Then in the vendor system, the holder is prompted to give his fingerprint in the scanner which is then sent to the server for comparison, if there is a match, the transaction is continued else it is rejected.

The traditional fingerprint recognition approaches are of two types: minutiae based methods and image based methods. The minutiae-based methods use feature vectors extracted from the finger prints and stored as set of points in the multi dimensional plane. The feature vector may contain feature of minutia point such as their positions, orientations and types. It is essentially required to find the best alignment between the features of minutiae in templates and those in fingerprints given under verification [2]. The disadvantages of minutiae-based methods are high computational complexities and they may not utilize the rich discriminatory information available in the fingerprints [4]. Whereas image-based methods use different types of features, such as their local orientation and frequencies rich shapes and texture information. The features extracted are more reliable than minutiae based method. In order to improve the matching accuracy even for rotated inputs, each fingerprint with ten associated templates with different angles is used. Hence these methods require a larger storage space and high processing time as well as the performance degradation due to the approximation. Transform method proposed for the matching with the input images in the database has not considered the invariance in input conditions. The fingerprint recognition using geometric moments with the learning vector quantization neural network too cannot deal with fingerprint image of which a reference point is located near its rim and its features obtained by a ROI (region of Interest) also cannot reduce the effect of nonlinear distortions.

The most useful descriptors for image representation and feature extraction are Geometric moments and Zernike moments, which are invariance to scale position and rotation. Some comparisons of them are listed below:

1) Domain: Geometric are calculated from the original image while, Zernike moments are calculated from the frequency domain. Zernike moments need to select the appropriate maximum number of order by trail experiments, while the geometric moments, avoid doing this than Zernike moments in this situation.

2) Stability: Geometric moments, are represented as image intrinsic properties, such as area, centroid so they have strong representation ability, however, geometric moments are vulnerable to noises due to easy variations of their numerical values, while Zernike moments are immune to noises.

3) Complexity: Geometric moments are simple and fast, while Zernike moments are more

From the above comparison, it is seen that both the geometric and Zernike moments have merits and demerits to represent the image. To overcome the shortcomings of the individual one, assembling the geometric moments and Zernike moments may be an effective way as well as improving the performances of the system. In order to ensure security to the user and authentication to the card in the cloud computing communications, a fingerprint recognition scheme based
on a set of assembled geometric moment and Zernike moment features for user content protection is proposed. The performance of the fingerprint recognition may be greatly affected by the complex input conditions such as image rotation, incomplete input image, poor quality image enrollment and so on. Both the geometric moments and Zernike moments are invariant to scale, position, and rotation, so they are able to handle the various inputs condition changed by affine transformations [6]. The geometric moment is used to extract features from the ROI whereas the Zernike moment is used to extract features from multiple ROI. Support Vector Machine (SVM) is a powerful classifier which can be used to assign the inputs to the corresponding class and verify the fingerprint inputs by matching feature vectors with those of template images.

In the proposed method, a fingerprint image is first preprocessed to enhance an original image by an enhancement method and it helps to localize the reference point. A unique reference point is determined on each fingerprint image by the complex filtering methods, regardless of the type of fingerprint, including a partial fingerprint. The complex filter is applied to ridge orientation field image to detect a reference point with the maximum curvature. The geometric and the Zernike moment features are extracted from the sub-ROIs region centered at a reference point in the enhanced image. These invariant features from a region adjusted by its orientation field can improve the time-consuming alignment of transformation and rotation occurred at other methods. It also significantly reduces the effects from noise and nonlinear distortions, and thus better preserves the local information. The contribution of this paper is that the fingerprint recognition scheme is based on effective preprocessing method and the extraction of features from the fingerprint image and matching process to ensure authentication, thus it able to handle various input conditions encountered in the cloud computing communications.

Off-Line Processing

V. FEATURE EXTRACTION

The method uses two stages: the offline stage and the online stage as shown in Fig. 2. In offline stage, the images are pre-processed by feature extraction module and then their extracted features are stored as templates in the database. In the online stage, the fingerprint image to be verified is first processed by feature extraction module; its extracted features are then fed to the matching module with one’s identity ID, which matches them against one’s own templates in the database. The feature extraction module is same in both the stages where the fingerprint image is given as input and then the next process includes five main steps as shown in Fig. 3 image enhancement, determination of reference point, determination of ROI and partition, assembling of invariant moment analysis, and PCA analysis.

A. Image enhancement

Short Time Fourier Transform (STFT) analysis is used to enhance the input fingerprint image. The quality of the input image is used to determine the performance of the fingerprint recognition system. The quality of the image is based on the clarity of the ridge structure in the fingerprint image. Image enhancement is done to improve the clarity of the ridge structure of the image. The intrinsic properties like local ridge orientation and local ridge frequency, foreground region mask are estimated by the algorithm and these properties are used to enhance the fingerprint image. Therefore, the image enhancement is done completely.

![Feature extraction flowchart](image-url)
B. Determination of reference point

The second step is to accurately and reliably determine the position of the reference point. It is necessary to consistently locate for unique reference point from all types of finger prints including partial finger prints. The reference point is the point of maximum curvature on the convex ridge [7]. It is usually located in the central area of the finger print. In the proposed method instead of determining the reference point from the original image, the reference point is determined from the enhanced image. Because the reliability and accuracy of detection is increased in the enhanced image. The complex filtering method is used for robust and reliable detection of the reference point in the finger print image.

C. Determination of ROI and Partition

Instead of using the entire finger print for feature extraction, speed of the overall process can be increased by using only a predefined area i.e. Region of Interest (ROI) around the reference point of the finger print image. Determined ROI region is divided into multiple sub ROIs which is done to reduce the effect of noise and nonlinear distraction and also to cover both the local and global information of the finger print image.

D. Assembling invariant moment and PC analysis

The Next process is the geometric moment and Zernike moments analysis which are applied on each sub ROI. Instead of using the gray level image the geometric and Zernike moment features are extracted from the binary image. This is because the binary image has stronger region representation ability than gray-level image. Each gray-level sub ROI is first binarized by applying local thresholds and then geometric and Zernike moment are computed from each sub ROI.

The PCA analysis is one of the oldest and the best known techniques in multivariate analysis [8]. The PCA analysis selects the most distinct features and reduces the dimension of features. The next process is the matching with SVM i.e. support vector machine. SVM is used to verify a matching between the input finger print images of those with template finger print that is stored in the database. The SVM indicates whether the input finger print matches with the stored finger print image in the database.

VI. EXPERIMENTAL RESULTS

The cloud database used in this experiment is the Xeround database. The bank uses its own cloud server and database to maintain the details of their customers but for the experimental purpose we use xeround cloud database. The plan of the xeround database can be changed easily whenever there is a need for larger storages.

Fig. 4 shows the xeround cloud database. For our experimental purpose of storing minimum samples 10MB is more than sufficient so we are using free plan of 10MB. The xeround database stores the fingerprint and the card holder details and maintains the database for each card holder.

![Fig. 4: Xeround cloud database](image_url)
the credit card terminal and then the fingerprint is scanned using the fingerprint scanner. The payment amount is entered in the host system. Both the credit card number and the fingerprint image is sent to the cloud database, the stored fingerprint image of the corresponding credit card number is taken and is compared with the original fingerprint image. If there is a match the transaction is proceeded as shown in Fig. 5 else the transaction is rejected.

Fig. 5 : Payment process and authentication verification

VII. CONCLUSIONS AND FUTURE WORK

The incidences of credit card frauds have increased with more card usage. The need of the hour is a dependable secure mechanism to reduce fraud in credit card usage. The current authentication systems were found to be rather inadequate. A system based on biometric fingerprint authorization integrated with cloud computing is being proposed and discussed from a technical perspective to emphasize its dependability. The obvious benefit of the proposed system includes reduced risk of authentication against card cloning, card theft and identity theft in the form of signature duplication and reduces forgery. As the proposed system overcomes the shortcomings of the existing credit card issue, it is viable in the immediate future.

The future work is to encrypt the fingerprint image and store it in the cloud database rather than storing the fingerprint image directly. The fingerprint image is then decrypted when the credit card is used during the transaction process and the verification is done, thereby it reduces the storage space in the cloud database. Further works include the improvement of performance and to reduce the storage space.

VIII. REFERENCES