Efficient Finger Print Authentication on Mobile Cloud Computing-A Survey

M. Malarmathi[1] M. Lalli[2]
[1,2]Bharathidasan university, Trichy

Abstract— Fingerprint Identification is a widely used Biometric Identification scheme. In biometric system, the fingerprint identification has been researched for the long period of time and it has shown the most promising future in the real world appliance. However, because of the composite distortions among the different impression of the same finger in real life, fingerprint recognition is still a demanding trouble. Matching two fingerprints can be unsuccessful due to various reasons and also depends upon the method that is being used for matching. Fingerprint (FP) serves to identify that the person authenticating is who he/she claim to be. FP identification is popular biometric technique due to easiness in acquiring, availability of prosperity sources for collecting data and their established use. A new feature for fingerprint images is introduced. This new attribute is named as Distance Vector. A Distance Vector count the minutiae points in each row of a particular fingerprint image. A Distance Vector is related with every fingerprint in the database. At the time of employment this feature is stored with the concerned fingerprint and at the time of matching this feature is matched with the Distance Vector of each fingerprint in the pattern database. This process increases the reliability of the fingerprint recognition task. In the initial stages, image normalization and orientation of the ridges are estimated. The system was evaluated using a standard fingerprint dataset and good performance and accuracy were achieved under certain image quality requirements. In addition, the proposed scheme was compared favorably to that of the state of the art systems.

Key words: Mobile Cloud Computing, Authentication, Fingerprint Matching, Minutiae Matching, Feature Vector Distance

I. INTRODUCTION

Cloud computing is that the delivery of computing as a service instead of a product, whereby shared resources, software, and knowledge area unit provided to computers and alternative devices as a utility (like the electricity grid) over a network (typically the Internet) Cloud computing depends on sharing of resources to attain coherence and economies of scale, like a utility (like the electricity grid) over a network. At the muse of cloud computing is that the broader construct of converged infrastructure and shared services.

Cloud computing, or in easier shorthand simply "the cloud", conjointly focuses on maximizing the effectiveness of the shared resources. Cloud resources area unit typically not solely shared by multiple users however also are dynamically reallocated per demand. this could work for allocating resources to users. as an example, a cloud laptop facility that serves With cloud computing, multiple users will access one server to retrieve and update their knowledge while not getting licenses for various applications.

Cloud computing exhibits the following key characteristics:

- Agility improves with users' ability to re-provision technological infrastructure resources.
- Application programming interface (API) accessibility to software system that allows machines to act with cloud software system within the same approach that a standard computer programmer (e.g., a laptop desktop) facilitates interaction between humans and computers.
- Cost**:** cloud suppliers claim that computing prices cut back. A public-cloud delivery model converts cost to operational expenditure. This supposedly lowers barriers to entry, as infrastructure is often provided by a 3rd party and doesn't to be purchased for one-time or sporadic intensive computing tasks. Evaluation on a utility computing basis is fine-grained, with usage-based choices and fewer IT skills area unit needed for implementation (in-house). The e-FISCAL project's progressive repository contains many articles trying into value aspects in additional detail, most of them last that prices savings depend upon the sort of activities supported and also the form of infrastructure offered in-house.
- Device and site independence change users to access systems employing an applications programmer notwithstanding their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the web, users will connect from anyplace.
- Maintenance of cloud computing applications is less complicated, as a result of they are doing not ought to be put in on every user's laptop and may be accessed from completely different places.

Cloud computing refers to associate degree on - demand, self - service web infrastructure that permits users to access computing resources from anyplace and anytime. The services offered by a cloud are often categorized into software system as a Service, Platform as a Service, Infrastructure as a Service, and Storage as a Service so on. Readying of a cloud falls into 3 sorts, viz. public, personal and community cloud. in an exceedingly public cloud, resources area unit receptive the overall public over the web. a non-public cloud infrastructure is operated for one organization. Once the resources area unit shared among organizations with common considerations, then it becomes a community cloud. the power to access knowledge and applications from anyplace and at any time with low value area unit the foremost vital advantages of mobile cloud computing.

The primary security issue on mobile cloud computing is protective remote knowledge and application s from illegitimate access. Whereas approved users will access the info, the cloud supplier can even do thus. There's additionally the likelihood of unauthorized access, which is

access by third parties like hackers. Therefore, the safety issue in mobile cloud computing becomes one in all the highest areas for analysis. In tradition, cloud computing users will avoid the safety risk by simply encrypting the info before it's sent and keep within the cloud. However, this is often not the case with the mobile users, as a result of secret writing technology isn't appropriate for mobile devices because of the secret writing method, which needs high work and high central processing. Fingerprint recognition has been widely used in both forensic and civilian applications. Compared with other biometrics features, fingerprint-based biometrics is the most proven technique and has the largest market shares. In terms of applications, there are two kinds of fingerprint recognition systems: verification and identification.

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae. The minutiae ending and bifurcation are shown in the Figure 1. A ridge ending is defined as the ridge point where a ridge ends abruptly. A bifurcation is defined as the ridge point where a ridge bifurcates into two ridges. It is a widely accepted assumption that the minutiae pattern of each finger is unique and does not change during one's life. When human fingerprint experts determine if two fingerprints are from the same finger, the matching degree between two minutiae pattern is one of the most important factors. Thanks to the similarity to the way of human fingerprint experts and compactness of templates, the minutiae-based matching method is the most widely studied matching method. The algorithms which are compared in this paper belong to the minutiae-based matching method.

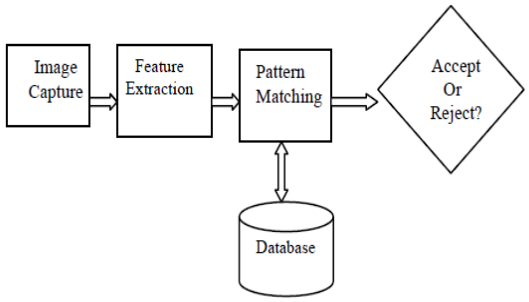

Fig. 1: Biometric System

A fingerprint recognition system operates either in verification mode or in identification mode. In verification, the input is a query fingerprint and an identity (ID). The system verifies whether the ID is consistent with the fingerprint. The output is an answer of yes or no. In identification, the input is only a query fingerprint and the system tries to answer the question: Are there any fingerprints in the database that resemble the query fingerprint? The output is a short list of fingerprints. Although fingerprint recognition has been studied for many years and much progress has been made, the performance of even state-of-the-art matchers is still much lower than the expectations of people and theory estimation. Therefore, much effort is still needed to improve both the performance and the speed of fingerprint recognition systems. The matching algorithm plays a key role in a fingerprint recognition system.

In this paper a new mechanism is proposed and implemented to authenticate mobile cloud computing by using fingerprint recognition as part of the security solution. Improving the mechanism of protecting access to the mobile cloud leads to improving the security overall, which at least protects the mobile cloud from unauthorized access. This section starts with an introduction to mobile cloud computing and describes the concept of mobile cloud computing.

II. Related Works

In this paper (2) Raju Sonavane , Dr. Sawant they describes exploitation the calculable orientation field, the input fingerprint image is adaptively increased within the recoverable regions A technology for recognizing fingerprints for security functions is proving as regards as reliable however economical recognition is counting on the standard of input fingerprint image. Recognition of the fingerprint becomes a posh pc drawback whereas managing droning and caliber pictures. During this Paper work we have a tendency to area unit focusing the special domain biometric System of droning and caliber pictures, which can be helpful for recognition system. Experimental results show that our improvement ways improves the performance of the fingerprint pictures makes it additional strong with relevance the standard of input.

In this paper (4) Md. Mamunur Rashid and Aktar Hossain they describes the projected Fingerprint Identification and verification System is identity verification methodology that uses digital imaging technology to get, store, and analyze fingerprint knowledge. Here we wish introduced a replacement methodology for fingerprint identification technology by trivialities feature extraction exploitation back-propagation formula. For Associate in input image, the native ridge orientation is calculable and therefore the region of interest is found. Then, ridges area unit extracted from the input image, refined to induce eliminate the tiny speckles and holes, and weakened to get eight -connected single wide ridges. Trivialities area unit extracted from the weakened ridges and refined exploitation some heuristics. A feature extractor finds point options like ridge finish, bifurcation, short ridge and spur from the input fingerprint pictures. The digital values of those options area unit applied to input of the neural network for coaching purpose. For fingerprint recognition, the verification a part of the system identifies the fingerprint based mostly coaching performance of the network. Finally experimental result show that the amount of recognized sample rate of our projected methodology is ninety fifth that is far higher than the prevailing fingerprint verification system exploitation artificial neural network (92.5%).

In this paper (8) B. Y. Hiew, A. B. J. Teoh, and O. S. Yin, they describes the preprocessing ways embrace key purpose location, finger image segmentation and fingerprint region extraction. Firstly, the key points together with fingertips and natural depression points, that area unit referred to as key points, area unit settled from the hand contour image. Secondly, the center finger is cropped from the hand image supported the knowledge of the key points' positions and therefore the knuckle's texture close to the finger root. Finally, the fingerprint is extracted from the center finger through the primary knuckle's texture.

attributable to the low resolution of the fingerprint pictures, linear projection ways like Principle part Analysis (PCA) and Linear Discriminator Analysis (LDA) area unit used for fingerprint feature extraction. Experimental results on a info of eighty six hands (10 impressions per hand) show that these approaches area unit effective.

In this paper (13) C. Lee, S. Lee, J. Kim, and S. J. Kim they describes a preprocessing algorithmic program of a fingerprint image captured with a mobile camera is projected. Fingerprint pictures from a mobile camera square measure totally different from pictures from standard or touch-based sensors like optical, capacitive, and thermal sensors. as an example, pictures from a mobile camera square measure colored and therefore the backgrounds or non-finger regions may be terribly erratic looking on however the image captures time and place. Also, the distinction between the ridges and valleys of pictures from a mobile camera is below that of pictures from touch-based sensors. due to these variations between the input pictures, a replacement and changed fingerprint preprocessing algorithmic program is needed for fingerprint recognition once victimization pictures captured with a mobile camera.

In this paper (11) A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee hey describes loud computing is combination of assorted computing entities, globally separated, however electronically connected. Because the Geographic of computation is moving towards company server rooms, it brings additional problems as well as security, like virtualization security, distributed computing, application security, identity management, access management and authentication. However, robust user authentication is that the preponderating demands for cloud computing that prohibit access of cloud server. During this regard, this paper proposes a powerful user authentication framework for cloud computing, wherever user legitimacy is powerfully verified before enter into the cloud. The projected framework provides identity management, mutual authentication, session key institution between the users and therefore the cloud server. A user wills amendment his/her watchword, whenever demanded. Moreover, security analysis realizes the practicableness of the projected framework for cloud computing and achieves potency.

III. OBJECTIVE

The objective of this Paper is to research the present techniques for fingerprint recognition. This target is chiefly rotten into image pre-processing, feature extraction and have match. For each sub-task, some classical and up-to-date methods in literatures are analyzed. Based on the analysis, an integrated solution for fingerprint recognition is developed for demonstration. For the program, some optimization at coding level and algorithm level are proposed to improve the performance of fingerprint recognition system.

A. DESCRIPTION OF THE PROPOSED SCHEME

The planned security model has a position over different models that offer single finger print system. The rationale is that, once associate interloper gains access to a finger print guide, he will claim to be associate attested user. Fingerprint algorithms incorporate 2 main phases, entering and identification or verification. The entering part, initial determines the worldwide pattern of the print, therefore it is classified during a massive bucket throughout improve matching performance, the point points ar then remodeled by a, generally proprietary, algorithmic program into a guide. The guide is hold on and used for future identification. a further step within the entering method might be to go looking for existing matches. This ends up in a stimulating advantage fingerprint authentication has over countersign authentication. Similarly as being proof of being a selected person, fingerprint identification may be used prove someone isn't a selected person or persons, like on a terrorist watch list, or antecedently having applied a profit.

Finger Print sample recognition process:

The recognition method at real time application. During this figure left fingerprint is at real time and right fingerprint is hold on in information. This figure shows completely different vector position at different points on finger. If the patterns hold on in information match with the important time pattern then it'll acknowledge otherwise it'll not acknowledge the person. The identification section, 1st determines a pattern bucket, and so submits the detail or template, betting on the look, which might be compared to the saved template. The comparison is completed with a applied mathematics analysis, since a particular match isn't expected. Matches are also found by rotating or translating the image, to catch up on the finger not being placed in the same location on every use.

Matching phase:

In this phase, a legitimate user is validated and an eavesdropper is invalidated. Even if the stored templates are hacked, the order of providing the impressions varies with the random number generated. Thus by means of trial and error, if a hacker tries with different permutations, access will be denied after three consecutive wrong attempts. The user has to reset the numbering that was earlier assigned. This phase also includes a method of reassignment of a biometric template along with numbers and mappings when the existing one, assumed to be compromised after three consecutive wrong attempts.

Fig 2. Fingerprint Matching

IV. ADVANTAGES OF FINGERPRINT AUTHENTICATION

Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

Utilization and efficiency improvements for systems that are often only 10–20% utilized.

Performance is monitored and reliable and loosely coupled architectures are constructed using web services as the system interface.

Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to set up application software upgrades to their computer.

Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Security can improve as a result of centralization of knowledge, inflated security-focused resources, etc., however issues will persist regarding loss of management over bound sensitive information, and therefore the lack of security for hold on kernels. Security is usually nearly as good as or higher than alternative ancient systems, partly as a result of supplier's area unit able to devote resources to determination security problems that several customers cannot afford to tackle. However, the complexness of security is greatly inflated once information is distributed over a wider space or over a bigger range of devices, likewise as in multi-tenant systems shared by unrelated users. Additionally, user access to security audit logs could also be troublesome or not possible. Non-public cloud installations area unit partly intended by users' want to retain management over the infrastructure and avoid losing management of knowledge security.

V. CONCLUSION

The combination of the cloud computing and mobile computing creates mobile cloud computing and additionally introduce security threats like unauthorized users access. the main focus during this analysis is on the mobile cloud and protective mobile cloud resources from illegitimate access. Biometric recognition is going to be utilized in the close to future in mobile devices. The projected resolution for authenticating mobile cloud users victimization the present mobile device camera as a fingerprint device to get a fingerprint image, so method it and acknowledge it. Results show that the projected resolution has additional price to stay performance at associate accepted level. For future work, accessing log file are going to be accustomed facilitate distinguishing unauthorized tries to access information by third parties–the cloud supplier or any intruders. Supported these logs, cloud security policies are going to be changed and re-configured.

REFERENCE

[1] www.wikipedia.com/fingerprint
[2] Raju Sonavane , Dr. Sawant, B. S., 2007, "Noisy Fingerprint Image Enhancement Technique for Image Analysis: A Structure Similarity Measure Approach", IJCSNS, VOL.7 No.9.
[3] Anil Jain, Sharath Pankanti, 1988, "Automated Fingerprint Identification and Imaging Systems". Technical Report 500-89, National Bureau of Standards.
[4] Md. Mamunur Rashid and Aktar Hossain, A. K. M., 2006, "Fingerprint Verification System Using Artificial Neural Network". (ISSIN 1812-5638)Information Technology Journal 5(6):1063-1067.
[5] Afsar, F. A., Arif, M., and Hussain, M., 2004, "Fingerprint Identification and Verification System using Minutiae Matching". National Conference on Emerging Technologies.
[6] Chaur-Chin Chen and Yaw-Yi Wang, 2003, An AFIS Using Fingerprint Classification (Palmerston North, November 2003).
[7] Jain, A.K., and et al, 2004, "An Introduction to Biometric Recognition", IEEE Tran. On Circuits and Systems for Video Technology, vol.14 No.1, PP. 4-20.
[8] B. Y. Hiew, A. B. J. Teoh, and O. S. Yin, "A secure digital camera based fingerprint verification system," Journal of Visual Communication and Image Representation, vol. 21, pp. 219-231, 2010.
[9] B. Hiew, A. B. J. Teoh, and D. C. L. Ngo, "Preprocessing of fingerprint images captured with a digital camera," in Control, Automation, Robotics and Vision, 2006. ICARCV'06. 9th International Conference on, 2006, pp. 1-6.
[10] P. Yu, D. Xu, H. Li, and H. Zhou, "Fingerprint image preprocessing based on whole-hand image captured by digital camera," in Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on, 2009, pp. 1-4.
[11] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, 2011, pp. 110-115.
[12] C. Lee, S. Lee, and J. Kim, "A study of touchless fingerprint recognition system," Structural, Syntactic, and Statistical Pattern Recognition, pp. 358-365, 2006.
[13] C. Lee, S. Lee, J. Kim, and S. J. Kim, "Preprocessing of a fingerprint image captured with a mobile camera," Advances in Biometrics, pp. 348-355, 2005.
[14] B. Hiew, A. B. J. Teoh, and D. C. L. Ngo, "Automatic digital camera based fingerprint image preprocessing," in Computer Graphics, Imaging and Visualizations, 2006 International Conference on, 2006, pp. 182-189.

