International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 38778-38784
© Research India Publications. http://www.ripublication.com

Deployment and analysis of Fingerprint Data using cloud services

Harneet Kaur
PG Scholar, Dept. of Information Technolgy, Guru Nanak Dev Engg. College Ludhiana District
er.harneet50@gmail.com

Sukhjit Singh Sehra
Assistant Professor, Dept. of Computer Science and Engineering Guru Nanak Dev Engg. College, Ludhiana District
sukhjitsehra@gmail.com

Sumeet Kaur Sehra
Assistant Professor, Dept. of Computer Science and Engineering Guru Nanak Dev Engg. College, Ludhiana District
sumeetksehra@gmail.com

Abstract
Over ensuing few years the number of biometric information being at the disposal of varied agencies and authentication service suppliers is anticipated to grow considerably. Such quantities of information need not only huge amounts of storage however unexampled process power likewise. To be ready to face this future challenges additional and additional square measure trying towards cloud computing, which may address these challenges quite effectively with its apparently unlimited storage capability, fast information, distribution and processing capabilities. Since the offered literature on a way to implement cloud based biometric services is extraordinarily scarce, this paper capitalizes on the foremost necessary challenges encountered throughout the event work on biometric services, presents the analysis of the fingerprint data by using cloud services. In this work, fingerprints are collected of 100 to 10 million people and processing is done on cloud only. A new methodology is explained in which firstly data is uploaded on the server and then the images which we want to compare is uploaded. Then its size and RGB of each pixel is compared. If the match found, then the resultant image is returned to the client.

Keywords— biometrics, cloud computing, fingerprint recognition, SaaS, MCC

Introduction

The number of web based services which are available commercially is developing quickly these days. Specifically, cloud computing gives an effective and financial method of conveying resources of Information technology (IT) on demand, and is relied to discover broad applications as technologies of virtualization and bandwidth of network keep on progressing. However, cloud computing introduces the industry of IT with energizing opportunities as well as with critical challenges since customers are hesitant to embrace solutions of cloud computing without firm guarantees in regards to security of their information. Two primary problems arise when clients applying cloud computing to software as a service (SaaS). Initially, if data of enterprise is to be prepared in the cloud, it must be encrypted to guarantee its privacy. Subsequently, proficient schemes of key management are obliged to encourage the tasks of encryption and relating decryption. Second, as the refinement of the tools utilized by malicious clients keeps on expanding, the information which is processed in the cloud is at expanding danger of attack. Therefore, there is a critical necessity for schemes of robust authentication to guarantee that the information can be accessed by users which are authorized and legitimate only. [1]

Cloud is a distributed computing which processes information which is distributed by the method of virtualization. At the point when consumer of cloud requests for computing infrastructure and resources, cloud gives it to the customers. To give ideal services for users of mobile it is one of major trends of technology of mobile in the future. Mobile cloud computing offers benefits of both cloud computing and mobile computing. For the improvement of applications of mobile the idea of cloud computing gives another opportunity as it permits the mobile devices to keep up a layer for client applications and shift the overhead of processing and computation to the virtual environment. Because of the availability of services and resources to access the MCC at any time and from anyplace and as a result of it, the issues of security overcame. There are few basic issues which are issued by MCC, such as potential attacks, personal data management, authentication of identity and privacy. The issues of security are the significant issues in the environment of cloud computing. To take care of such types of the problems of security a method of authentication is proposed known as biometric identification in which biometric manages the physical characters of the human body such as retina scanning, palm print, finger print etc. [2]

Biometrics are said to be the most ideal method of authentication which is made by utilization of behavioural and physical characteristics, for example, tongue, voice, facial, iris, fingerprint etc. By utilizing this technique, user herself/himself can only having access to their system. In this way, no method for unlawful authentication can be conceivable. The systems are utilized to permit access depending upon the identification of biometric. This enhances the security level in the system than the passwords usage.

Cloud computing is the developing technology of conveying numerous sorts of resources as services, primarily over the Internet. Biometrics in the Cloud implies that the whole infrastructure of biometrics of business is placed in the hands of the facilitating supplier, and is accessible on the interest.

This incorporates the servers which have the database of biometric template, the connectivity of the network to the business, and the greater part of the processing which happen keeping in mind the end goal to conduct the transactions for identification and verification which are necessary. This system keeps the most serious issue with authentication,

(i) by utilizing same passwords and username to many sites,
(ii) misuse of the password,
(iii) for-getting the passwords. [3]

Cloud computing has evolved as a noteworthy platform that gives a mixed services on a pay for every model usage. It gives services at application, platform and software layer. The US National Institute of Standards and Technology (NIST) have caught five crucial characteristics of cloud: measured service, resource pooling, ubiquitous network access, rapid elasticity and on-demand self-service. There are mainly two types of cloud: Data Cloud and Compute Cloud. The cloud which gives services related to storage is called data cloud. The cloud which gives service related computing power is under the compute cloud. Both of these service models of cloud have distinctive requirements as for their security. For example, securing a compute cloud mostly incorporate detection of sequences of system call, trojans, malwares that are focusing to disturb the computational efficiency given by the vendor of cloud, whereas securing an information will certainly concentrate on attacks which are based on network that may attempt to get access to information which is unauthorized and stored in it. [4]

The remaining paper is framed as follows. In Section 2 some introduction about fingerprint recognition is given. In Section 3 the existing literature related to biometrics in the cloud is surveyed and various differences have been done with this paper. In Section 4 problem formulation of fingerprint analysis and objectives of research work is explained. In Section 5 research methodology is provided. In Section 5 results are presented and screenshots are given and, finally, the paper is summarized with some final comments and directions for future work in Section 6.

Fingerprint Recognition

Fingerprint recognition has been utilized generally as a part of both civilian and forensic applications. When contrasted to features of biometrics, biometric which is based on fingerprint is the most mark based biometrics and has the largest shares of market. As far as applications, there are mainly two kinds of systems of fingerprint recognition: verification and identification. A fingerprint is the pattern of valleys and ridges on the surface of the tip of finger. The crossing points and end points of ridges are known as minutiae. A ridge ending is characterized as the point of ridge where a ridge ends unexpectedly. A bifurcation is characterized as the point of ridge in which ridge bifurcates into two ridges. It is an assumption which is accepted widely that the pattern of minutiae of every finger is unique and does not change during one's life. At the point when experts of human fingerprint figure out whether two fingerprints are from the same finger, the degree of matching between two patterns of minutiae is standout amongst the most essential features. [5]

Fingerprint recognition is one of the well known and powerful methodologies for priori approving the users and securing the elements of information when communication is taking place. Normally, approaches of conventional fingerprint recognition are categorized into two classifications: minutiae based methods and image based methods. In the methods which are based on minutiae, feature vector may have components of minutia points, for example, types, orientations and positions. The main disadvantage of this type is that they might not use the information which is discriminatory rich and accessible in the fingerprints and may have high complexity of computation. On another hand, methods which are image based utilize distinctive sort of features which are gotten from patterns of ridge of fingerprint. For example, their shapes of ridge, information of texture and frequencies and local orientations. The features may be separated out more reliably than distinguishing minutiae from fingerprints. Among several methods which are image based, a Gabor filter which is method of feature based demonstrated moderately high performance contrasting with different works which are done previously, these strategies obliged a large space for storage and a relatively high performance time and also the degradation of performance because of the approximation. The performance of fingerprint recognition may be significantly influenced by the input conditions which are complex, for example, enrollment of image of poor quality, incomplete input image, image rotation etc. Both the Zernike moments and geometric moments are invariant to rotation, position and scale, so they find themselves to manage various conditions of input.

Related Work

Lots of research work has been done in the analysis and verification of fingerprint data. Some of the important work is described as follows:

In Reference [7], authors proposed a secured key generation algorithm using fingerprint based biometric modality. Biometrics is used in high secure applications for natural, user-friendly and quick authentication. Cryptography makes sure the secrecy and authenticity of message but protecting the confidentiality of the cryptographic keys is the major problem to be dealt with. Researchers suggest using biometric options to get sturdy and repeatable cryptographic keys rather than a memorable password. The combination of biometrics with cryptography solved this problem. This paper present ways to generate the strong bio-crypt key based on fingerprint. Fingerprint biometric modality is predominant due to its two characteristics uniqueness and permanence that's ability to stay unchanged over the lifetime.

Paper [8] describes a new method to verify fingerprints. A research purpose is to verify integral transformations applying possibilities using Fourier and Fourier-Mellin transformation as a tool for fingerprints images verification. The proposed method does not require broad preprocessing, it eliminates partly inaccurate finger place on a sensor (shift, rotation), it compensates partly fingerprint deformations (scale change, skin elasticity) and lower fingers quality (too dry fingers),

automatic processing and evaluation is done without an operator input. The proposed method, using a registration and comparative criterion of modified phase correlation can take up 91.7 % of the right fingerprints and reject just 8.3 % of them. The fingerprint verification can be used to follow and control technological processes; expensive or dangerous equipments, technologies or property protection from illegitimate using or misusage, and for an authentication of entry into buildings.

In Reference [9], about biometric authentication as a service on cloud is explained. Biometrics is more reliable to authenticate user's behavior than the traditional means of password authentication.Since Biometric identification is unique and slow, it provide the solution to ensure that the rendered services are accessed only by a legitimate user and no one else. Biometric systems identify users based on behavioral or physiological characteristics. The advantages of these systems over traditional authentication methods, such as passwords and IDs, are well known. Hence, biometric systems are more beneficial in terms of usage. As security is the main concern in using cloud computing fused biometric authentication technique which can be used as single sign on. Doing this, services can be more secure and reliable and biometric authentication is provided as a service by a cloud provider.

In Reference [10], authors talked about fingerprint verification using cloud services. Cloud-computing services are being offered by various organizations recently. Peer-to-Peer (P2P) networks can be used to solve computationally intensive problems in collaboration with computing environment. In this work, PC cluster is used to simulate a P2P network and present results of a computationally intensive image matching algorithm (fingerprint verification). Collective communications are used to transfer images to destination peers over a network. Communication to computation time ratio is calculated by transferring of fingerprint images of various sizes on the internet. As transfer of raw images is communication intensive, an alternative method is used which involves FBI approved Wavelet Scalar Quantization (WSQ) compression method at the source before transmitting to the destination nodes. The viability of fingerprint identification and/or verification service is studied offered by cloud computing. In particular, a distributed fingerprint verification algorithm is presented.

Paper [11] presents a secure mobile computing based on fingerprint. Cloud computing is a new paradigm shift to manage computing offers, are scalable, secured, high available computation resources and software as a service enable the users to access to cloud services from anywhere and anytime. Mobile Cloud Computing (MCC) describes the availability of Cloud Computing (CC) services in a mobile environment and combined with heterogeneous fields like mobile phone device, cloud computing & wireless networks. MCC is become the buzzword and a major discussion thread in the IT world in these days. In this paper a new effective model is designed to solve the identification problem in MCC. The proposed solution is based on the fingerprints to prove the users identity to determine whether the user is authorized or not. Each fingerprint is combined with a password to form a multiple passwords scheme. The password consists from the finger sequence in the hand (left or right) plus a fixed password, makes the passwords easy to remember. The results showed that this scheme is reported to be very strong and difficult to break.

Motivation

Among all the modalities of biometric, identification based on fingerprint is the oldest methodology that has been employed successfully in various applications. Fingerprints are one in all the foremost developed technologies of biometric and additionally considered real evidences of verification in courts of law over the place in the planet. Therefore, fingerprints are utilized in divisions of forensic worldwide for investigations related to criminal. The basic idea is to collect fingerprints of various people and it may range from 100 to 10 million. The data will be stored on the cloud, processing and analyzing will be done only online. End user have capability to examine the data they have collected as much faster rate as before because earlier method has various problems like:

(i) Due to large data missing of critical time window will lead to slowness of computer.
(ii) The application which are already in use require prior training and they are hard to use.

The objectives of our research work are as follows:

1. Implementation of fingerprint matching algorithm on localhost.
2. Deployment of cloud "Infrastructure as a Service".
3. Implementation of fingerprint matching algorithm on cloud.
4. Validating results.

Proposed Scheme

Generally today more research is focused upon the community cloud and public cloud and FAAS is present in Community cloud.

We will over here deal with little part of forensic i.e. Biometric. Our Plan is that there is:

1) Lot of difficulty to police in order to find the previous criminal record of person.
2) They have to run through various or bulk of files.

The steps used in methodology are as given below:

1. Firstly there is folder on the cloud server named as Upload Files. where all our uploaded files are store i.e. the finger prints that we have uploaded on the server.
2. In the folder of Upload Files, there is another folder named as Temp which gets into action when we try to match finger prints on the server.
3. Now whenever we upload the finger prints out images will be stored on the cloud server in Upload Files Directory.
4. When we try to compare the finger prints on to the server then our finger print first uploaded in to the Temp Directory of the Cloud server in Upload Files.

How the Server compares fingerprints:
When File is Successfully Uploaded to the Test Drive for matching then we send secret keys to perform the Finger Print Matching operation.

How the Server works:
1. First when the server receives the request then the server loads all the images from the upload files into the array and the image we want to compare is loaded in the particular image object on the server.
2. Then the whole array items are iterated one by one. We have used the Java RGB methodology to compare finger prints.

How RGB methodology works:
1. First image from the array is picked up and the image to compare is picked up. As the first we compare the sizes of these two images and then as guided and internet research we found that we can say two images are 100% equal if their every pixel matches each other.
2. So after comparing the size of these images and we find the RGB of each pixel of both the images and each pixel RGB is matched with required finger print.
3. As the RGB fails we go to the next array iterate item and then checks other. As the RGB are matching as the complete image is matched and then it return the index that matched successfully that matches and then first server tells that this index is matched and then it returns the resulted image into result panel on the client window.

For Comparison of time:
First when the user select the image to compare time is selected and when the server returns the results then again the time is selected and then the time difference is computed and shown to the user that this much time is taken to show results from the server. The flowchart is as shown below:

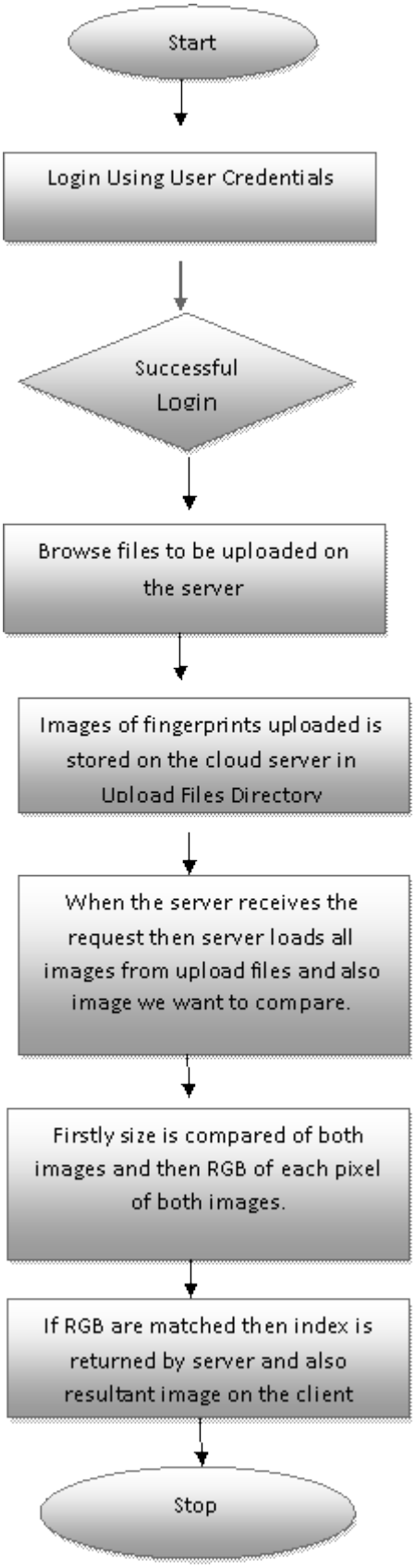


Fig. 1 Flowchart of proposed work

Simulation

This section presents the simulated results of analysis of fingerprint data by using cloud computing.

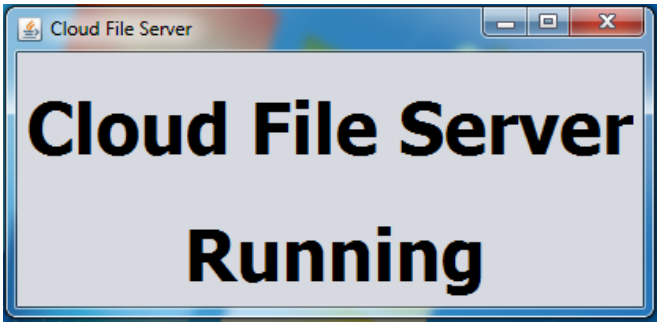
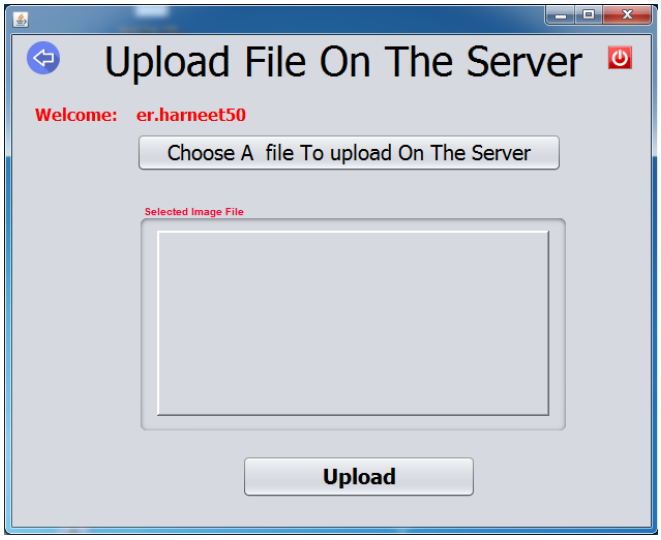
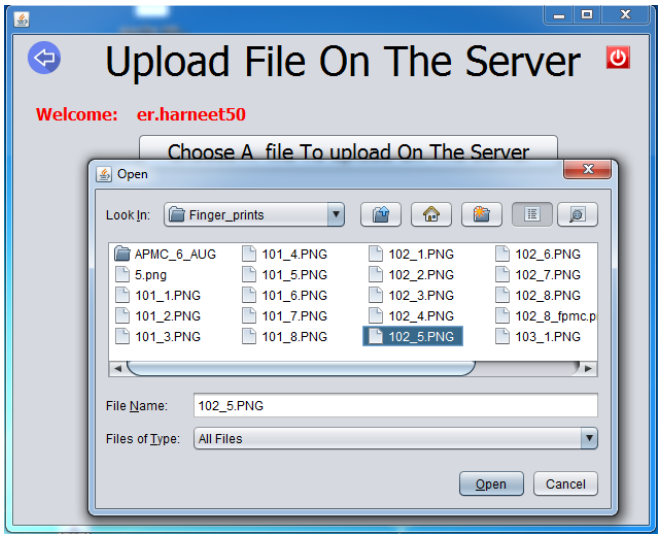
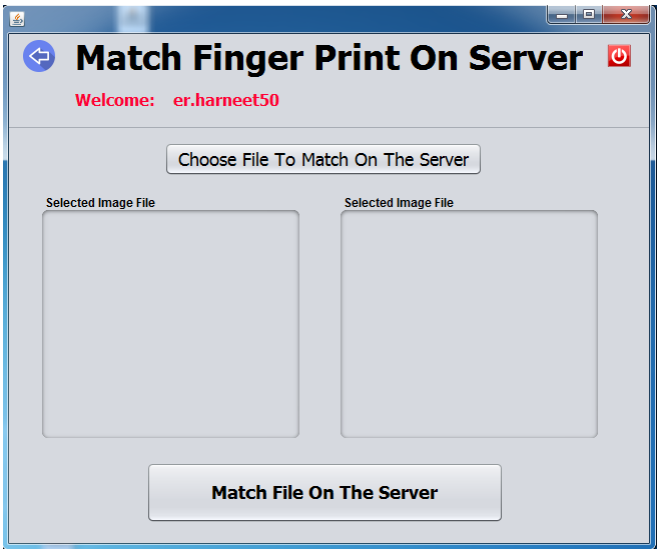


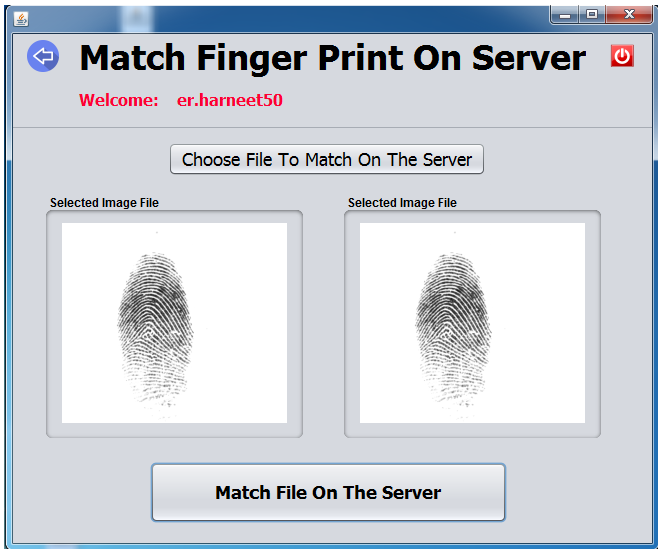
Figure:- At Server side:- Cloud Server is Running

Figure:-At Client Side:-We match fingerprint









Conclusion

In this paper we have described a methodology for fingerprint matching. The fingerprints are uploaded on the server first.

And after that, the image we want to compare is matched by the server by matching the size and RGB of each pixel of both the images. And then the result is conveyed to the user. The main advantages of this work are there will be better management of employees in Govt. Sector and also there will be decrease in fraudulent cases and also decrease in crime. Time is also computed and then it is shown to the user also how much time is taken by the server.

Acknowledgement
The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible

References

[1] Ping Wang, Chih-Chiang Ku, Tzu Chia Wang, "A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security", National Cheng Kung University, Taiwan.

[2] Nileshree R. Darve, Deepti P. Theng, "Image Processing on Eye Image Using SURF Feature Extraction", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 4, April 2015.

[3] K. Srividhya, Mr. S.V. Manikanthan, "A Comparative Analysis of Raspberry Based Metric Using Cloud Computing Techniques", International Journal of Emerging Technology in Computer Science & Electronics (IJ.. ETCSE), Vol. 13, Issue 2, March 2015.

[4] Sanchika Gupta, Anjali Sardana, Padam Kumar, Ajith Abraham, "A Fingerprinting System Calls Approach for Intrusion Detection in a Cloud Environment", Indian Institute of Technology, Roorkee, Uttarakhand, India.

[5] D. Ashok Kumar, T. Ummal Sariba Begum, "A Comparative Study on Fingerprint Matching Algorithms for EVM", Journal of Computer Sciences and Applications, Vol. 1, No.4, 2013.

[6] Supriya Wable, Chaitali Laulkar, "Fingerprint Recognition Scheme using Assembling Invariant Moments and SVM", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.

[7] A. Jaya Lakshmi, I. Ramesh Babu, "Design of Secured Key Generation Algorithm using Fingerprint Based Biometric Modality", IOSR Journal of Engineering (IOSRJEN), Vol. 2, Issue 2, pp: 325-330, February 2012.

[8] P.Alena, B. Pavol, "Industrial production surety factor increasing by a system of fingerprint verification", International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), Vol. 1, April 2014.

[9] Himabindu Vallabhu, R V Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution", International Journal of Soft Computing and Engineering (IJSCE), Vol. 2 Issue 4, September 2012.

[10] Fazal Noor, Majed Alhaisoni, Antonio Liotta, "Fingerprint Verification using Cloud Services with Message Passing Interface over PC Clusters", Fourth International Conference on Advances in P2P Systems, 2012.

[11] Alaa Hussein Al-Hamami, Jalal Yousef AL- Juneidi, "Secure Mobile Cloud Computing Based-On Fingerprint", World of Computer Science and Information Technology Journal (WCSIT), Vol. 5, No. 2, 2015.

[12] IehabALRassan, HananAlShaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security & Its Applications, Vol. 5, No. 6, 2013.

[13] Soweon Yoon, Jianjiang Feng, Anil K. Jain, "Altered Fingerprints: Analysis and Detection" IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.34, 2012.

[14] K. Govinda, Yannick Ngabirano, "Secure Data Storage in Cloud Environment Using Biometrics", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 5, May 2012.

[15] Padma. V, Geetha. P, Ramya. G, "Fast Access Control (FAC) using Fingerprint Identification in Cloud Computing", International Journal of Research in Engineering & Advanced Technology, Vol. 1, Issue 1, March 2013.