AUTHENTICATION AND AUTHORIZATION CONTROL IN COMPUTATIONAL GRID ENVIRONMENT USING FINGERPRINT MINUTIAE FEATURE AND ATTRIBUTE BASED ACCESS CONTROL

[1] AbdulRaheem Muyideen, [1] Tomori R. A., [2] Jimoh R. G., [3] Salimonu I. R.

[1]COMSIT Directorate, University of Ilorin, Ilorin, Nigeria
[2]Department of Computer Science, University of Ilorin, Ilorin, Nigeria
[3]Department of Computer Science, Federal Polytechnic, Offa, Nigeria

Corresponding Author: Jimoh R. G., jimoh_rasheed@yahoo.com

***ABSTRACT*:** Computational Grids is highly heterogeneous shared resources for problem solving in any dynamic environment. Accepting Grid computing technologies will be difficult, unless users are certain of safety of their data like in their own environment. Security in Computational Grids is in two folds. Security of the grid users ensuring authentication, confidentiality, integrity, single sign on and delegation on one hand and security of the grid resources in the form of authorization and access control on the other hand. Existing methods of authentication in computational grids have proved inadequate for identifying users; hence, a more reliable technique is required. This paper provides a model, which allows users reliable transactions in grid by using fingerprint to enhance security in grid. Thus, this study aimed at hybridizing fingerprint biometric and Attribute Based Access Control (ABAC) for authenticating and authorizing computational grid users based on attributes of the users for computational grid resources.
KEYWORDS: authentication, authorization, grids, biometric, security

1. INTRODUCTION

Ian and Carl ([IC98]) defined computational grid as a fittings and software foundation that gives reliable, predictable, pervasive, and reasonable access to top of the line computational capacities while Oracle describes computational grids in simple term, as the gathering of all IT resources into one set of collective services for the whole of big project computing needs. In their definition, Ali, et al. ([A+02]) described computational grids infrastructure as constant analysis of grid resources and adjusts supply accordingly. Computational grid involves virtualization of dispersed processing assets, for example, handling system transfer speed, and capacity ability to make a solitary framework picture, allowing users and applications consistent access to limitless IT abilities. According to Marty and Mary ([MM01]), Computational Grid is gathering of heterogeneous machines and assets distributed over various regulatory spaces for clients to have access to these assets with ease. The availability of these assets in space poses a serious threat which call for authentication and authorisation of the assets users, giving clients simple access to these assets.

Authentication is the power to figure out if an individual, application, server, or other element is, indeed, who or what it is pronounced to be. There are several authentication methods such as use of biometric, password, one-time pad, kerberos and so on. Authentication is achieved through presenting something you are – a biological trait (a biometric), something you know – passwords, something you own – digital certificates, tokens, smart cards and keys; and personal identification numbers (PIN). Biometrics authentication is considered highly secured and attractive alternative as a result of difficulty in forging or stealing someone traits. It is even harder than stealing personal information such as a PIN or password. Neither can they be given to another user nor be forgotten by the user. In most cases, they are ease and do not present any burden to the end user.

Attribute Based Access Control is an idea to shift the standard of allowing particular user to access resource to estimating client's attributes for resource access. Instead at the point of authentication, a choice is made focused on the estimation of particular traits whether access ought to be accepted or not. Attribute-based system provides access control and authorization utilizing advanced coarse, scalable and semantically rich methodology ([YT05]). Service supplier (SP) describes policies that state the set of attributes needed for using its services. The user on the other hand, gives credentials that have attributes verifiable to gain access to these services. Several levels of access can be granted based on attribute values of the user. This methodology is considered useful for computational grid, where keeping real time synchronization in access control lists is a serious problem ([Nag01]) and not knowing previous information of the user at the service supplier.

According to Ravi ([Rav06]) and Adewole ([Ade13]), there are seven major biometric technologies in existence today. They are: Signature recognition, Keystroke recognition, Voice recognition, Fingerprint recognition, Iris and retina recognition, Facial recognition and Hand geometry recognition. Out of these technologies, iris recognition, hand geometry recognition and fingerprint recognition are widely in use.

The remaining of the paper is organised as follows: Section 2 describes Fingerprint Minutiae. Section 3 discusses related work. Section 4 focuses on the methodology and section 5 is the result and conclusion.

2. FINGERPRINT MINUTIAE FEATURES

Generally, fingerprint consists of two kind of features: global features, and local features. Global features comprise of right loop, left loop, whorl, arch and tented arch. Local features comprises of spur, lake, island crossover bifurcation and ending. Figure 1 show various minutiae types.

Figure 1: Common minutiae types

The two most widely used features of the fingerprint are the ridge ending in which a ridge ends suddenly and bifurcation in which a ridge branches into two or more as presented in the Figure 2. Fingerprints were accepted as one of the main biometrics technologies for personal identification trustworthiness. Fingerprints is hard to forge, and unique to every individual fingerprint.

Figure 2: Fingerprint features

Today, majority of grid systems rely on Grid Security Infrastructure for security, which make use of public key infrastructure (PKI) and proxy certificate ([MS10]). PKI uses public key based authentication and encryption. Each grid user possesses a public key and private key that need to be kept safe. At the centre of PKI is the certificate, which is used to identify the user and the public key associated with the user. Certificate Authority (CA) issues the certificate to user. As more users participate in the grid so is the quantity of public and private key generated increases as well as the certificate issues. The management of the certificate becomes a serious problem. As a result of this, difficulty in managing, distributing and revoking compromised keys in Grid Security Infrastructure systems is generating an obstacle to wide use and adoption of Grid system ([BJC06]). Thus, a number of studies have revealed the need to introduce a more secured Grid environment as a significant requirement to make grid systems available in different commercial applications. Therefore, this research work intends to shift paradigm from PKI cryptographic-based methods of securing grid using a hybridized fingerprint biometric and Attribute Based Access Control models that provides authentication of users and authorization of resources in grid environments.

3. RELATED WORKS

In computational grid, users and providers depend on the trustworthness of one another. That is the users is satisfied by the ability of the providers and at the same time providers is sensibly content with and ready to give service to the users. To accomplish this sort of dependable transactions shared trust must be created between the users and the providers. To achieve this, Srivaramangai and Renagaramanujam gave in 2010 a model which permits just dependable transactions in grid by utilizing trust as a measure for both users and providers.

To address the security risks connected with the grid, Ali, Sumalatha, Nirav, Rimato, Renato, and Jose ([A+02]) proposed two level methodology to the security of the grid. First level to handle interactive shell sessions, and second level to handle randomly user-submitted applications. The methodology comprises of a limited shell and a system-call checking module. The shell consists of a standard command shell amplified with a security module that keenly checks the orders issued by the network user. These check authorize the host security policy. The result of the first level is controlled by the second level. Ali et al. ([A+02]) based their second level on processing based ability given by the ptrace systems-call and the proc file-system as gave in UNIX and LINUX systems which permits a parent process to keep a look at its child process and adjust the conduct of the child process. For their system, execution performance analysis gives up to 2.14 times execution overhead progress for shell-based applications. The methodology proves efficient and gives a substrate to hybrid procedures that consolidate static and dynamic mechanisms systems to minimize monitoring overheads.

Ian, Carl, Gene, and Steven ([I+98]) analyzed the notable security requirement of the computational grid and created a security policy and corresponding security architecture. The policy according to Ian, et. al. ([I+98]) dealt with single sign-on, interoperability with local policies, and dynamically varying resource requirements. This approach concentrated on authentication of users, resources, and processes and supports user-resource, resource-user, process-resource, and process-process authentication. The researchers depicted a security architecture modeling and related protocol that actualize the approach inside the Globus metacomputing toolbox. Beckles et. al., ([B+06]) observed that current security model for computational grid is complicated to utilize and exorbitant to execute. The researchers proposed an easy to use security model for computational grid environment.

Vipul, Omkant, Amit and Brent ([V+06]) created security system utilizing Key Policy Attribute-Based Encryption. The researchers relate private key with access structure that determines which kind of ciphertexts the key can decode. In that capacity each user's key is connected with a tree-access structure where the leaves are connected with attributes. A user can decode a ciphertext if the attributes connected with a ciphertext fulfill the key's access structure. Urs and Peter ([UP05]) proposed proof-based access-control archtectural scheme that uses hierarchical identity-based encryption services in pervasive environment to covertly notify users without releasing data of the obliged proof of access. Likewise, the researchers present and actualize an encryption-based access-control archtectural that make use of hierarchical identity-based encryption with a specific end goal to manage multiple, hierarchical obligations on access rights. Also Wang and Wang in 2007 combined public key cryptography CPK employing elliptic curve cryptography ECC to achieve authentication in grid.

In this paper, we introduce a different method, which rely on biometrics for authentication and ABAC for authorization of grid users.

4.1 METHODOLOGY

The focus of this study is to develop a hybrid system for authenticating and authorizing users of computational grid. The study intends to achieve its objectives through the implementation of the various stages involved in fingerprint authentication such as fingerprint image acquisition, fingerprint image enhancement, minutiae feature extraction, fingerprint template generation into two halves a card and database; and fingerprint template matching. Computational grid users' fingerprints are captured using fingerprint optical scanner. Successfully authenticated users were authorized through the stages of Attribute Based Access Control of PEP, PDP, PIP and PAP. The stages of fingerprint feature extraction are presented in Figure 3.

Two types of techniques used for capturing fingerprints are inked (off-line) and live-scan (ink-less). In inked fingerprints method, fingerprints are acquired traditionally by a qualified person who spreads a black ink into the individual's finger. Then, the finger is pressed against a paper card, which is later scanned to produce the digital image. The inked impression method remains popular especially in forensics. Furthermore, this type of technique is not feasible for biometric systems where real-time processing is required. Live-scan fingerprints are acquired by directly sensing the fingerprints over an electronic fingerprint device. Since the images are capture directly in digital format, no intermediate digitization process is required. This makes real-time biometric systems feasible. To authenticate user in this work, live-scan method is used to capture fingerprint of user in real time. Today, there are several live-scan fingerprint technologies available, however, important factor is to ensure good quality in the captured images using small, fast, and inexpensive scanning gadgets. The proposed System Framework is shown in Figure 4.

4.2 Fingerprint Image Acquisition

The initial phase in fingerprint recognition is image acquisition, which is the methodology of obtaining and digitizing fingerprint of individual user for further transformation. Customarily, the inked or off-line method has been utilized to obtain the fingerprint data from a user, however, today scan-live is the method normally use for certain application, for example, access control. The essential purpose behind the attractiveness of fingerprint recognition is the accessibility of experienced, advantageous and ease sensor that can quickly secure the fingerprint of client with least or no intervention of human operator. Optical scanner is the gadget utilized for fingerprint acquisition of users fingerprint for the purpose of this work.

Every individual user has only one kind fingerprint. A fingerprint is the outline of ridges and valleys on the fingertips. Unique fingerprint is hence characterized by the uniqueness of the local ridges attributes and their relationship. At the point when fingerprint is scanned, a ridge on the fingerprint is regarded as single curved segment, and a valley is the section between two nearby ridges. Minutiae points are the local ridge characteristics that exist either at a ridge ending or at a ridge bifurcation. The fingerprint image quality is critical for the execution of fingerprint recognition system. Numerous components may impact the unique fingerprint image quality, for example, the kind of sensor used to obtain the image (optical, capacitive), coarse fingertips (manual specialist, senior individuals, unfavorably susceptible skin), fingertip condition (wet, dry), image resolution (500 dpi,250 dpi), poor contact of the finger with the sensor, occurrence of noise, latent images traces from the past user.

Automatic minutiae detection is complex mission as consequence of existence of some of these elements bringing about low quality fingerprint images. Unique Fingerprint image improvement procedures are frequently utilized to lessen the noise and to improve clarity of ridges against valleys so that no spurious minutiae are recognized. Researchers have proposed many ways for improvement of Fingerprint image which include: image normalization and Gabor filtering ([HWJ98]), Enhancement of fingerprint Image by Short Time Fourier Transform (STFT) Analysis ([CCG05]), Binarization Method ([TJ95]), Directional Fourier filtering ([SMM94]), Enhancement using directional median filter ([WSG04]), Fingerprint image enhancement using dominant ridge direction technique ([KDB97]), using color histogram and textual features to retrieve Image ([CW11]) and some different other systems.

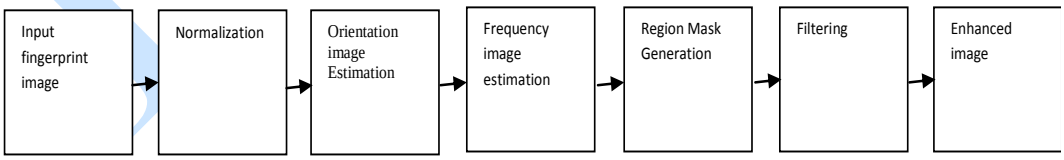

Figure 3: Fingerprint features

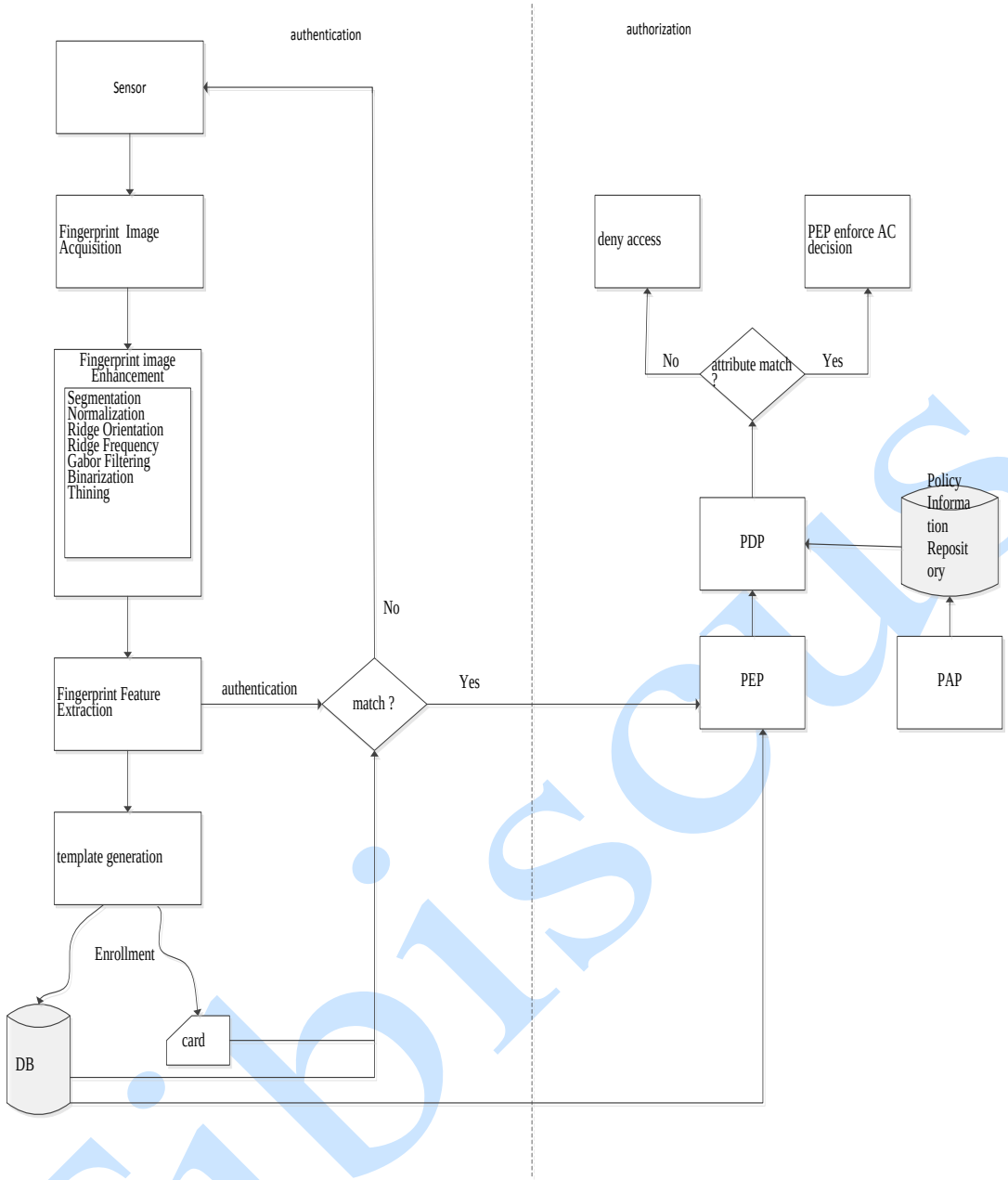

Figure 4: Proposed system framework

4.3 Image Enhancement

The essential characteristic of fingerprint image is the nature of the ridge structures it contains, because the ridge has the essential data needed for minutiae feature extraction. The act of minutiae feature extraction schemes and fingerprint recognition procedures vigorously depends on the quality of input fingerprint image. In a good quality fingerprint image, ridges and valleys swap and go in a direction consistently ([Ray03]). It is therefore, the objective of an improved scheme to enhance the ridges structures in the recoverable locales and imprint the unrecoverable region as excessively boisterous for subsequent operations. This enhancement encourages the discovery of ridges and subsequently, permits correct separation of minutiae from the thinned ridges. Practically, fingerprint image are not generally distinct because of factors of noise that degenerate the ridge structures quality. The ambiguity sometimes happens because of varieties in skin and impression conditions, for example, dirt, humidity, scars, and non-smooth contact with the gadget for capturing fingerprint. Accordingly, improvement of the fingerprint image is regularly utilized to decrease the noise and improve the quality of ridges and valleys. Several proposed techniques are in the literature for improvement of the fingerprint image. The usual methodology is the Gabor filtering which has four principal stages: (i) normalization, (ii) ridge orientation estimation, (iii) ridge frequency estimation and (iv) filtering. The researcher utilized the methodology by Raymond ([Ray03]) incorporating three extra stages with the four stages mentioned above which are segmentation, binarization and thinning for the fingerprint image improvement. Each of these stages is discussed in the subsequent section.

(a) Segmentation

Segmentation is the first phase in image enhancement algorithm. This is the procedure of isolating the foreground areas in the fingerprint image from the background areas. The foreground area coincides with the required clear

fingerprint region comprising the ridges and valleys, which is of concern. The background region coincides with the regions out of boundaries of the fingerprint region, which have no any substantial fingerprint data ([Ray03]). The background regions of fingerprint image in general have a low grey-scale variance value while the foreground regions have a very high variance value, thus, a system based on variance threshold is utilized to isolate the foreground from the background. In this technique, the image is separated into blocks in order to compute the grey-scale variance value of every block that formed the image. Suppose that the variance is below the global threshold, in that case the block is allocated background area; else, the block is allocated to the foreground. The grey-level variance of a block of size W x W image is given as:

$$V(k) = \frac{1}{W^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}\left(I(i,j) - M(k)\right)^2 \quad (4.1)$$

where *M(k)* is the mean grey-level value for block *k*, *I(i, j)* is the grey-level value at pixel *(i, j)* and *V(k)* is the variance for block *k*.

(b) Normalization

Once fingerprint image segmentation is completed, the next phase in image enhancement is normalization of image. Normalization is utilized to regulate the values of intensity in an image by fine-tuning the scope of grey-level values in order that it exists in the scope needed. Suppose that I(i, j) represents the grey-level value at pixel (i, j), and N(i, j) represent the normalized grey-level value at pixel (i, j). The normalized image is given by Raymond ([Ray03]) as:

$$N(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{V_0\,(I(i,j) - M)^2}{V}} & \text{if } I(i,j) > M, \\ M_0 - \sqrt{\dfrac{V_0\,(I(i,j) - M)^2}{V}} & I(i,j) \le M \end{cases} \quad (4.2)$$

where *M* and *V* are the estimated mean and variance of *I(i, j)* and M_0 and V_0 are the desired mean and variance values respectively.

(c) Ridge Orientation Estimation

Ridge orientation estimation of a fingerprint image consists of the local orientation of the ridges in the fingerprint as demonstrated in Figure 4.

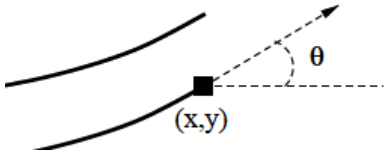

Figure 4: Fingerprint Ridge Orientation

Computing the estimate of this orientation is an extremely critical stage as the next Gabor filtering phase relies upon local orientation to adequately improve the fingerprint image. In the literature, several systems were proposed for ridge orientation estimation. Among these are the chaincode system proposed by Xudong and Wei-Yun ([XW00]), Stock and Swonger ([SS69]) utilized ridge valley mask with a set of number of reference templates (8 slits) to ascertain orientation field, Mehtre based strategy proposed by Mehtre et al. ([MMK87]) and the least mean square estimation strategy proposed by Hong et al. ([HWJ98]) which measure the orientation in a block-wise way. The researcher has picked the methodology utilized by Raymond ([Ray03]) which evaluates the orientation in a pixel-wise way. This will create an improved and more precise estimation of the orientation field. To compute the orientation field at pixel (i, j) utilizing pixel-wise methodology, the following steps given below are taken:

A block of size W x W is centered at pixel (*i, j*) in the normalized fingerprint image.

For every pixel in the block, calculate the gradients $\partial x(i,j)$ and $\partial y(i,j)$ which are the gradient value in the *x* and *y* directions, in that order. The horizontal Sobel operator is utilized to calculate $\partial x(i,j)$ and the vertical Sobel operator is utilized to calculate $\partial y(i,j)$.

The local orientation at pixel (*i, j*) can then be evaluated utilizing this mathematical equation:

$$V_x(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}}\sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2\partial_x(u,v)\partial_y(u,v) \quad (4.3)$$

$$V_y(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}}\sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} \partial_x^2(u,v)\partial_y^2(u,v) \quad (4.4)$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\frac{V_y(i,j)}{V_x(i,j)} \quad (4.5)$$

where $\theta(i,j)$ is the least square estimate of the local orientation at the block centered at pixel (*i, j*).

The orientation field is then smooth in a local region utilizing a Gaussian filter. The orientation is initially changed into a continuous vector field, which is given as:

$$\Phi_x(i,j) = \cos\left(2\theta(i,j)\right) \quad (4.6)$$

$$\Phi_y(i,j) = \sin\left(2\theta(i,j)\right) \quad (4.7)$$

Where Φ_x and Φ_y are the *x* and *y* components of the vector field, respectively. Gaussian smoothing is then performed after the vector field is estimated. This can be obtained as given:

$$\Phi_x'(i,j) = \sum_{u=-\frac{W_\Phi}{2}}^{\frac{W_\Phi}{2}}\sum_{u=-\frac{W_\Phi}{2}}^{\frac{W_\Phi}{2}} G(u,v)\,\Phi_x(i-uw, j-vw) \quad (4.8)$$

$$\Phi_y'(i,j) = \sum_{u=-\frac{W_\Phi}{2}}^{\frac{W_\Phi}{2}}\sum_{u=-\frac{W_\Phi}{2}}^{\frac{W_\Phi}{2}} G(u,v)\,\Phi_y(i-uw, j-vw) \quad (4.9)$$

where *G* is a Gaussian low-pass filter of size $w\Phi$ x $w\Phi$. The final step is to obtain the smooth orientation field *O* at pixel (*i, j*). This can be calculated as follows:

$$O(i,j) = \frac{1}{2}\tan^{-1}\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)} \quad (4.10)$$

(d) Ridge Frequency Estimation

The local ridge frequency is another fundamental parameter that is utilized by Gabor filter. This corresponds to the local frequency of the ridges in a fingerprint image. Separation of image into squares of size W x W is the initial phase in the frequency estimation. Following this is to extend the grey-level estimations of every pixel situated in each block in a direction orthogonal to the local ridge orientation. This estimation produces a practically sinusoidal-shape wave using the local minimum points relating to the fingerprint image ridges. The ridge spacing S(i, j) processed by calculating the average number of pixels in continuous minima points in the anticipated waveform. Accordingly, the ridge frequency F(i, j) of a block centered at pixel (i, j) is given as:

$$F(i,j) = \frac{1}{S(i,j)} \quad (4.11)$$

(e) Gabor Filtering

After the computation of ridge frequency and ridge orientation, the resulting parameters are utilized as a part of the Gabor filter. Gabor filter was utilized for this research on the grounds that it consists of orientation-selective and frequency-selective properties. The Gabor filter spatially used filter on the fingerprint image ([Ray03]). The orientation value O(i, j) and ridge frequency value F(i, j) of that pixel are needed by convolution of a pixel (i, j) in the image. In this way, improved image E obtained by applying the Gabor filter G is achieved as given below:

$$E(i,j) = \sum_{u=-\frac{w_x}{2}}^{\frac{w_x}{2}} \sum_{v=-\frac{w_y}{2}}^{\frac{w_y}{2}} G\left(u,v;O(i,j),F(i,j)\right)N(i-u,j-v) \quad (4.12)$$

where *O* is the orientation image, *F* is the ridge frequency image, *N* is the normalized fingerprint image, and w_x and w_y are the width and height of the Gabor filter mask, respectively.

(f) Binarization

Binarization transforms gray-scale image to binary image using threshold value. For a gray-scale fingerprint image, a pixel assumes 256 diverse intensity stages. According to ([PN13]), different methods utilized to transform gray-scale image to binary image in Global binarization includes Fixed Thresholding, Otsu and Kittler Methods. While Local binarization uses Niblack, Adaptive, Sauvola and Bernsen Methods.

On the other hand, Local Adaptive Thresholding strategy proposed by ([S+11]) was utilized in this research in line with the fact that, it safeguards valuable data in the fingerprint images different from global thresholding procedure that can damage the fingerprint image. In this method, the pixel values lower than the limit are given value zero and the intensity values more than the limit are given value one. For binary image, the pixel values got 0 and 1 representing black and white pixels in that order ([S+10]). Several minutiae extraction algorithms work on binarized fingerprint image in which the black pixels means ridges, and the white pixels means valleys in that order. This enhances the distinction between the fingerprint image ridges and valleys, and thus encourages the extraction of minutiae ([P+12]).

(a) (b)

Figure 5: (a) Improved gray-scale image; (b) Binarized image

(g) Thinning

Thinning is the final image enhancement stage commonly carried out before minutiae extraction takes place. Thinning is a morphological operation that progressively changes the foreground pixels into one pixel wide ([Ray03]). While forming a skeletonized variant of the binary image, the thinning algorithm is applied to a fingerprint image to conserve the integration of the ridge structures. Extraction of minutiae is then produced from the skeleton. Many strategies have been proposed by researchers to carry out fingerprint thinning. Some of these algorithms are Two-way Thinning Algorithm (TTA), Fast Thinning Algorithm (FTA), and Ridge Line Following Algorithm (RLF) ([Gha05]). Still, the researcher utilized Ridge Line Following Algorithm proposed by Emiroglu ([Emi97]) because of its accuracy in thinning a fingerprint image. Figure 6b demonstrates a thinned fingerprint image:

(a) (b)

Figure 6: Thinned fingerprint image: (a) Binarized image; (b) Thinned image

4.4 Fingerprint Image Minutiae Feature Extraction

Feature extraction comprises of bringing out the ridge endings and ridge bifurcations out of the fingerprint images data. Fingerprint matcher algorithms regularly being used are sensitive to precision of ridges and valleys, measures of nature and number of minutiae, and image size. Minutiae matching basically comprise of discovering the best configuration between the template of the minutiae in the database and a subset of minutiae in the input fingerprint through a geometric change. Usually each recognized minutiae m_i is represented by four parameters

$$m_i = (x_i, y_i, \theta_i, t_i) \quad (4.13)$$

Where

x_i, y_i - are the minutiae point coordinates

θ_i - is the angle minutiae make with the horizontal

t_i - is the type of minutiae point

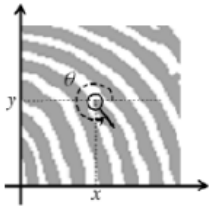

Figure 7: Ridge ending minutiae coordinate (x, y) and the minutiae orientation θ

There are many minutiae extraction techniques existing in the literature. They are broadly grouped into two: minutiae extraction techniques based on binarized fingerprint images and gray-scale fingerprint images. Cross Number Based technique is used for its computational effectiveness and intrinsic ease. This technique includes the utilization of the skeletonized image in which the ridge flow pattern is eight- connected. Minutiae extraction takes place by checking the nearby neighbourhood of every ridge pixel of the image utilizing a 3x3 window as indicated in figure 8.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 8: 3x3 Neighbourhood

The CN value can then calculated as follows:

$$CN = 0.5 \sum_{i=1}^{8} |p_i - p_{i+1}| \quad (4.14)$$

where $P_9 = P_1$.

It is calculated as half the summation of difference between pairs of adjacent pixels in the eight-neighbourhood. Utilizing the CN properties illustrated in figure 9, the ridge pixel is identified as a ridge ending, bifurcation or non-minutiae point. Take for instance, a ridge pixel having CN equal to one is considered as a ridge ending, while CN of value three is considered to be bifurcation.

CN	Property
4	Crossing point
3	Bifurcation point
2	Continuing ridge point
1	Ridge ending point
0	Isolated point

Figure 9: Properties of Crossing Number

Each of the extracted minutiae points has x and y coordinates, orientation of the corresponding ridge portion (θ), and the kind of minutiae. Figure 10 shows ridge ending and bifurcation and their Crossing Number values.

(a) **(b)**

Figure 10: (a) Ridge ending CN=1; (b) Bifurcation CN=3

4.5 Template Generation

Generally past stages often present some artifacts, which later become false minutiae. This false minutia will fundamentally influence the precision of matching in the event that they are just viewed as true minutia. Hence, techniques of evacuating false minutia are essential for efficient fingerprint verification system. The technique by ([MGR12]) is employed in this work for eradicate false minutia as given below:

Assume D is the mean between ridge widths is given as the mean separation between two parallel neighbouring ridges.

If the width between one bifurcation and one termination is less than D and the two minutiae are in the same ridge, get rid of both of them.

If the width between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations.

If two terminations are contained in width D and their directions are coincident with a small angle variation. Furthermore, they satisfy the condition that no other termination is between the two terminations. At that point, the two terminations are viewed as false minutia obtained from broken ridges and therefore removed.

Suppose two terminations are found in a short ridge with length within distance less than D, get rid of the two terminations.

This technique for false minutiae removal is advantageous because, firstly, ID of the ridge is utilized to recognize minutia and seven kinds of false minutia are concisely established when compared with other techniques. Also, the technique is well-structured to ease false minutiae recognition. It surpasses the method used by Intelligent biometric systems in fingerprint and face recognition that does not use the relations among the false minutia types.

After false minutiae are gotten rid of, Crossing Number CN is utilized for minutiae extraction of unique fingerprint image of users for this research. Unique finger impression Fingerprint Template is created from minutiae point extracted. Minutiae point extracted comprise of ridge ending and bifurcation. The ridge ending template is saved into a card while the bifurcation template is saved into the database together with user information of interest. The templates can then be referred to at the point of authentication.

4.6 Template Matching

In this step, we examine fingerprint matching, which is the responsible for contrasting an input fingerprint that is given by the user, to a template fingerprint that is given previously, at enrollment stage. In general fingerprint matching technique are minutiae based, these are the ridge endings and bifurcations of the fingerprint ridges.

Technique for minutiae-based fingerprint matching comprises of two steps, which are registration and counting of minutiae. In registration step, positioning of the fingerprint took place utilizing translation, rotation and scaling together while in minutiae counting step, the matching score is known by computing the related minutiae pairs that are available in the fingerprints. If a minutia from the test set is found inside a bounding box or tolerance zone around a minutia from the template set then the two minutiae are related. The matching score, in the range of 0 and 1, is computed as the quantity of matched minutiae over the cumulative number of minutiae.

Minutiae Matching technique: For this stage the fingerprint information is contrasted with the template information stored in the system. Information of the extracted minutiae is saved as a matrix of rows equivalent to minutiae points quantity, and with four columns: columns 1 is the column list of every minutiae point; columns 2 is the column index of every minutiae point; columns 3 is the orientation angle of every minutiae point; columns 4 is the type of minutiae (1 – ending, 2 – bifurcation, 3-normal ridge). At the matching process, every minutiae point is contrasted with the template information. There are many algorithms for contrasting minutiae. One of them changes template information points to polar coordinates utilizing the given equation below:

$$\begin{pmatrix} r_K^T \\ \\ \\ \phi_K^T \\ \\ \\ \theta_K^T \end{pmatrix} = \begin{pmatrix} \sqrt{\left(row_K^T - row_{ref}^T\right)^2 + \left(col_K^T - col_{ref}^T\right)^2} \\ \\ tan^{-1}\left(\dfrac{\left(row_K^T - row_{ref}^T\right)}{\left(row_K^T - row_{ref}^T\right)}\right) \\ \\ \theta_K^T - \theta_{ref}^T \end{pmatrix} \quad (4.15)$$

Where for template image

r_K^T radial distance of K^{th} minutiae

ϕ_K^T radial angle of K^{th} minutiae

θ_K^T orientation angle of K^{th} minutiae

row_{ref} , col_{ref} row index and column index of reference point presently under consideration

The information matrix points were changed to polar coordinates utilizing the mathematical equation:

$$\begin{pmatrix} r_m^I \\ \\ \\ \phi_m^I \\ \\ \\ \theta_m^I \end{pmatrix} = \begin{pmatrix} \sqrt{\left(row_m^I - row_{ref}^I\right)^2 + \left(col_m^I - col_{ref}^I\right)^2} \\ \\ tan^{-1}\left(\dfrac{\left(row_m^I - row_{ref}^I\right)}{\left(row_m^I - row_{ref}^I\right)}\right) + rotate\ value(k,m) \\ \\ \theta_m^I - \theta_{ref}^I \end{pmatrix} \quad (4.16)$$

rotate values = the difference between the orientation angles of T_k and I_m. T_k and I_m represent the extracted information in all the columns of row k and row m in the template and data matrices, respectively.

To compare two minutiae sets, T_1 is taken from template or saved fingerprint template and I_2 is from input fingerprint. T_1 and I_2 are said to be matched if their minutiae type are the same, their position and direction are close.

If $f^1 \in T1$, $f^2 \in I_2$ and

$$TYPE(f^1) = TYPE(f^2) \quad (4.17)$$

$$DIST(f^1, f^2) \leq D_f \quad (4.18)$$

$$ANGLE(f^1, f^2) \leq A_f \quad (4.19)$$

For this situation, (f1, f2) is a matched minutiae features. Df and Af are maximum tolerance for translation and rotation in that order. Let Sm be a set of matched pairs. Every component in Sm has the structure (f_i^1, f_i^2) where f_i^1 is from T_1 and f_i^2 is from I_2. There are two limitations of Sm. All f_i^1 and f_i^2 in *Sm* should be differ ([Gha05]). These imply that every minutia in T_1 or I_2 should not be matched more than once. The accompanying condition should likewise be fulfilled if (f_1^1, f_1^2) and (f_2^1, f_2^2) are two components in Sm.

$$| DIST(f_1^1, f_1^1) - DIST(f_2^2, f_2^2) | < \varepsilon \quad (4.20)$$

Where ε is a small value. The next process is to perform pairing and computation of similarity measure M as shown in equation 4.21:

$$M = \sqrt{\frac{N_m x N_m}{N_1 x N_2}} \quad (4.21)$$

Where N_m is the number of element in the match minutiae, N_1 is the number of elements in T_1 and N_2 is the number of elements in I_2. The algorithm is described in detail in this section.

Pattern based algorithms compare the essential fingerprint patterns template earlier saved and an input fingerprint. Thus, the images are adjusted, around a central point on each image in the same position. The input fingerprint image is contrasted graphically with the template in order to know matching level.

Correlation Based Technique: Suppose I(Δx, Δy, θ) is a rotation of the input image I by an angle θ around image center and moved by Δx and Δy pixels in the directions x and y, in that order. At that point the similitude between the two fingerprint images T and I was calculated as

$$S(T, I) = (_{\Delta x}, \Delta y, \theta^{max} CC\left(T, I^{\Delta x, \Delta y, \theta}\right) \quad (4.22)$$

Where CC(T, I) = $T^T I$ is the cross- correlation between T and I. The cross-correlation is a well known measurement of image relationship. It gives the optimal registration. Some drawback of this system are a) Non-linear distortion makes impressions of the same finger fundamentally differ regarding global structure; b) Skin condition and finger pressure create image intensity, complexity, and ridge thickness to oscillate essentially over distinctive impressions and c) The method is computationally extremely costly.

Image Based Techniques: Image based method do matching utilizing the global features of an entire fingerprint image. It is an improved developing technique for fingerprint recognition. This method incorporates both

optical and computer-based image correlation systems. In recent times, some transform-based methods have additionally been investigated. Phase-based fingerprint image matching system utilizing 2D discrete Fourier transforms proposed in Gabor filter based fingerprint matching strategy.

4.7 Storage of Template Generation

After successful registration of a user by the system and their template extracted, the template is saved so it might be recovered later for examination. Three fundamental ways of template storage are:
1. Store the template on a handy card.
2. Store the format at the biometric reading gadget
3. Store the template remotely in a unified database
The primary benefit of saving the templates inside the biometric reading gadget is quicker response time. Saving and recovery of little amount of templates might be taken care of adequately by most systems, however big amount of template create issues and will oblige better off storing template in a centralized database. Saving template in a centralized database brings about a noticeable improvement alternative for different systems. Extra resources are required to keep up with the extra the network traffic and system created in the biometric reader gadget and the database. The advantage of saving the template on a card is that the users will have control of the feature. They can as well utilize the card anywhere there is card reader device, making it more helpful for the provider to position card reader at various areas. The best storage solution is the usage of two storage systems that join together. This will take into consideration consolidated profits of the results and in the meantime nullify any of the potential hindrances.

4.8 Policy Information Repository

To saveguard the resources on the system we need to give the guidelines of who has the right to use the resources and what operations the user can perform on the resources. This set of guidelines is known as a policy. The Policy Information Repository PIR saves group of logical rules and policies that guide access choices. To secure the resources on the computational grid, it is required to point out the rules that state who has the right to access the resources and what operations the user can perform on the resources. Extensible Access Control Markup Language (XACML) XACML is the general policy language used to ensure resources and in addition a right to gain access decision language. It permits creation of policy rule with conditions as a logical representation joining together attributes of the subject and/or resources.

4.9 Matching Attribute

Matching attribute is policy assessment methodology which right to access resources rely on the security policy. Access Control Decision Function (ADF) controls the access by applying access control policy guidelines to access demand. The function is given by the relation below

$$p_{i_{adf}|attr(Req),Attr(Ser),Attr(Res),Attr(Act),Attr(Env)} = \begin{cases} Deny \\ \square \\ \square \\ Allow \end{cases}$$

Where

$p_{i_{adf}}$ is the ADF function for policy p_i
$attr(Re, q)$ is the attributes the requestor
$Attr(Ser)$ is the service
$Attr(Re, s)$ is attribute of the resource
$Attr(Act)$ is the action
$Attr(Env)$ is the environment.

5. Results and Discussion

In this section, the various results obtained from the proposed system after executing the stages involved were fully discussed. The entry point to the proposed system is the user identification interface. After the identification interface, the user enters details about him/herself and the enrolment interface. An attacker attempting to attack the model will need the two factors used for the model that is, card and the fingerprint. The card can be stolen but without the fingerprint, the attacker cannot succeed in his mission. The model separated the fingerprint into two parts, therefore the attacker cannot have the two separated parts from the card if stolen. It is extremely difficult for an attacker to obtain the two authentication parameters for a particular user and hence the model is safe. As explained that the fingerprint is two and then stored in a card and the server respectively, the user information and privacy is equally protected since the information are not in plaintext. An unauthorized individual cannot be allowed into the system to use the resources since such user would not be able to bypass the authentication stage of the system.

6. Conclusion

It has been shown that the existing methods of securing the computational grid resource is inefficient and ineffective and the password can be compromised. There is need for a simplified, efficient and reliable model for managing computational grid resources based on fingerprint biometric and attribute based access control technologies. To achieve this, various stages involved in fingerprint authentication and attribute based access control were explored. A comprehensive discussion on each stage of the proposed framework were discussed. implemented. These include fingerprint image acquisition, segmentation, normalization, ridge orientation estimation, ridge frequency estimation, Gabor filtering, binarization, thinning, fingerprint feature extraction, fingerprint template generation, and fingerprint template matching for authentication and policy enforcement, policy decision and attribute policy information for authorization. Each of these stages has several methods that can be used to achieve them. The results have shown that fingerprint biometric is indeed a unique way of identifying user based on who he/she is. Biometric access is a better substitute for the use of username / password in identifying users. The genuineness of the fingerprint makes it a reliable access control technique. The fact that a user no longer needs to memorize password or write it down for identification

purpose has eased the use. The model is robust towards authentication, authorization and network attacks. Therefore, it provides efficient solution for enhancing the security of the grid computing.

REFERENCES

[Ade13] **K. S. Adewole - Development of Unilorin biometric Attendant System**. MSc Thesis, Ilorin. (Unpublished), 2013.

[A+02] **R. B. Ali, A. Sumalatha, H. K. Nirav, F. Rimato, F. Renato, A. B. Jose** - *Fine-Grain Access Control for Securing Shared Resources in Computational Grids*. Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'02). IEEE Computer Society, 2002.

[BJC06] **M. Baolin, S. Jizhou, Y. Ce** - *Reputation-based Trust Model in Grid Security System*. Journal of Communication and Computer, 3(8), 2006.

[B+06] **B. Beckles, P. V. Coveney, P. Y. Ryan, A. E. Abdallah, S. M. Pickles, J. M. Brooke, M. McKeown** - *A user-friendly approach to computational grid security*. Proceedings of the UK e-Science All Hands Meeting, 2006.

[CW11] **Chuen-Horng L., Wei-Chih L.** – *Image Retrieval System based on Adaptive Color Histogram and Texture Features*. The Computer Journal vol. 54 Issue 7, 2011.

[CCG05] **Sharat S. Chikkerur, Alexander N. Cartwright, Venu Govindaraju** - *Fingerprint image enhancement using STFT analysis*. Advances in Pattern Recognition - ICAPR, pp. 20-29, 2005.

[Emi97] **I. Emiroglu** - *Fingerprint Image Enhancement and Recognition*. Ph.D Thesis, University of Hertfordshire, Department of Electrical and Electronic Engineering, 1997.

[Gha05] **B. S. Ghazali** - *Design and Development of an Automated Fingerprint Verification System*. 2005. Retrieved November 15th, 2013, from http://www.eprints.utm.my/4348/1/74021.pdf.

[HK09] **K. Hisham, S. A. Khaled** - *Adapting and accelerating the Stream Cipher Algorithm "RC4" using "Ultra Gridsec" and "HIMAN" and use it to secure "HIMAN" Data*. Journal of Information Assurance and Security, 2009.

[HWJ98] **L. Hong, Y. Wan, A. K. Jain** - *Fingerprint image enhancement: Algorithm and performance evaluation*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 777-789, 1998.

[IC98] **F. Ian, K. Carl** - *The Grid: Blueprint for a Future Computing Infrastructure*, 1998.

[I+98] **F. Ian, K. Carl, T. Gene, T. Steven** - *A Security Architecture for Computational Grids*. 5th Conference on Computer and Communications Security. San Francisco CA USA: ACM, 1998.

[KDB97] **S. Kasaei, M. Deriche and B. Boashash** - *Fingerprint feature extraction using block-direction on reconstructed images*. TENCON '97. IEEE Region 10 Annual Conference. Speech and Image Technologies for Computing and Telecommunications., Proceedings of IEEE, Brisbane, Qld., Australia, 1997.

[MM01] **H. Marty, R. T. Mary** - *Security Implications of Typical Grid Computing Usage Scenarios*. 10th IEEE International Symposium. High Performance Distributed Computing, 2001.

[MS10] **A. J. Mohamed, M. Satoshi** - *Authorization within Grid-Computing Using Certificateless*, 2010.

[MGR12] **A., K. Meenakshi, S. Gaganpreet, R. Ravi**. - *Minutiae Feature Based Algorithm for Finger Print Recognition and Verification*. VSRD-International Journal of Electrical Electronic and Communication Engineering 279-287, 2012.

[MMK05] **H. Marty, R. T. Mary, R. J. Keith** - *Security for Grids*. Proceedings of the IEEE, 93 (3), 2005.

[MMK87] **B. M. Mehtre, N. N. Murthy, S. Kapoor** - *Segmentation of Fingerprint Images using the Directional image Pattern Recognition*. 429-435, 1987.

[Nag01] **S. Nagaraj** - *Access control in distributed object systems: Problems with access control lists*. IEEE WETICE, 2001.

[PN13] **G. Puneet, K., G. Naresh** - Binarization Techniques used for Grey Scale Images. *International Journal of Computer Applications Volume 71– No.1, 2013.*

[P+12] **B. Pankaj, B. Kishore, N. A. Mohammad, Mohammed W. R.** - *Fingerprint Image Enhancement and Its Feature Extraction for Recognition*. International Journal of Scientific and Technology Research, 117 - 121, 2012.

[Rav06] **D. Ravi** - *An introduction to biometrics: A concise overview of the most important biometric technologies*. Keesing Journal of Documents & Identity, 2006.

[Ray03] **T. Raymond** - *Fingerprint Image Enhancement and Minutiae Extraction*, 2003.

[RS09] **V. Ruckmani, S. G. Sadasivam** - *A novel trigon-based dual authentication protocol for enhancing security in grid environment*. International Journal of Computer Science and Information Security, 6(3), 64 - 72, 2009.

[SS69] **R. Stock, C. Swonger** - *Development and evaluation of a reader of fingerprint minutiae*. Technical Report XM-2478-X1, Cornell Aeronautical Laboratory, 1969.

[S+10] **Shashikumar, D. R., Kumar, K., Raja, K. B., Chhotaray, R. K., & Pattnaik, S**. - *Hybrid Fingerprint Matching Using Block Filter and Strength Factors.* In Computer Engineering and Applications (ICCEA), 2010 Second International Conference. IEEE.

[SMM95] **B. G. Sherlock, D. M. Monro, K. Millard** – *Fingerprint enhancement by directional Fourier filtering*, IEE Proc.-Vis. Image Signal Process., Vol. 141, No. 2, 1994.

[S+11] **T. Romen Singh, Sudipta Roy, O. Imocha Singh, Tejmani Sinam, Kh. Manglem Singh** - *A New Local Adaptive Thresholding Technique in Binarization*. International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011.

[TJ95] **Øivind Due Trier, Ani K. Jain** - *Goal-Directed Evaluation of Binarization Methods*. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 17, no 12, 1995.

[UP05] **H. Urs, S. Peter** - *Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information*. Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.

[V+06] **G. Vipul, P. Omkant, S. Amit, W. Brent** - *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*. ACM Conference on Computer and Communications Security, 2006.

[XW00] **J. Xudong, Y. Wei-Yun** - *Fingerprint minutiae matching based on the local and global structures*. Proc. of International Conference on Pattern Recognition (ICPR), (pp. 1038-1041), 2000.

[YT05] **E. Yuan, J. Tong** - *Attribute based access control (ABAC) for web*. Proceedings OF THE IEEE International Conference on Web Services, 2005.

[WSG05] **C. Wu, Z. Shi, V. Govindaraju** – *Fingerprint image enhancement method using directional median filter*. Proc. SPIE 5404, Biometric Technology for Human Identification, 2004.