Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing Database Records through Conceding User Roles Based on Human Authentication

Richa Sharma*, Vinit Kumar
Computer Science and AKTU, Uttar Pradesh,
India

Abstract: ***Data is the most significant and essential entity to every organization. Companies invest millions of dollars in order to protect and manage the access to their data. Now-a-days, companies take utmost precautionary measures in order to safeguard the data not only from any external attacks but also from unauthorized access from within the organization. The databases are designed in such a manner that they are being assigned different roles which govern the access to records. Amongst the various measures which are adopted to secure the data records, we have planned to implement the concept of identifying and authenticating the physical features of humans which access the data. In other words, we validate and restrict the access to the database according to the roles assigned to human beings for records accessibility, the basis of their facial features. As we know, the data is accessed and managed through functions which apply various calculative actions on the records. For ex: Data can be manipulated through, insertion of fresh data, modification of existing data or deletion. In order to assign these functions, we need to create roles for the users who may access these functions via the roles assigned to them and through this application, we propose to assign and authenticate these roles through the recognition of facial data:***

Keywords: ***Facial Recognition, Database Security, Eigen Faces, Eigen values, Eigen vectors, Principle component analysis.***

I. INTRODUCTION

Data is the most significant and essential entity to every organization. Companies invest millions of dollars in order to protect and manage the access to their data. The privacy and confidentiality of any data could be easily determined from the fact that the sensitivity of organizational data is because of its profit figures, business revenues, client details, etc. If this data falls into the wrong hands or rivals and is being misused, organizations can have to bear a heavy loss and pay a penalty for that.

The databases are designed in such a manner that they are being assigned different roles which govern the access to records. For ex: In the very first place, databases are normalized and then different tables have accesses according to the role of a user. In other words, more experienced users have a deeper access to the database records whereas less experienced employees access only the surface information.

Traditionally databases have been largely secured against hackers through network security measures such as firewalls, and network-based intrusion detection systems. While network security controls remain valuable in this regard, securing the database systems themselves, and the programs/functions and data within them, has arguably become more critical as networks are increasingly opened to wider access, in particular access from the Internet.

Furthermore, system, program, function and data access controls, along with the associated user identification, authentication and rights management functions, have always been important to limit and in some cases log the activities of authorized users and administrators. In other words, these are complementary approaches to database security, working from both the outside-in and the inside-out as it were.

Many orgnizations develop their own baseline security standards and designs detailing basic security control measures for their database systems. These may reflect general information security requirements or obligations imposed by corporate information security policies and applicable laws and regulations e.g. concerning privacy, financial management and reporting systems, along with generally-accepted good database security practices such as appropriate hardening of the underlying systems and perhaps security recommendations from the relevant database system and software vendors.

II. TECHNIQUE USED

A. Microsoft visual c++

Microsoft Visual C++ (often abbreviated as MSVC or VC++) is a commercial (free version available), integrated development environment (IDE) product from Microsoft for the C, C++, and C++/CLI programming languages. It features tools for developing and debugging C++ code, especially code written for the Microsoft Windows API, the DirectX API, and the Microsoft .NET Framework A set of Eigen faces can be generated by performing a mathematical

process called principal component analysis (PCA) on a large set of images depicting different human faces. Informally, Eigen faces can be considered a set of "standardized face ingredients", derived from statistical analysis of many pictures of faces. Any human face can be considered to be a combination of these standard faces.

B. Eigen faces

A set of Eigen faces can be generated by performing a mathematical process called principal component analysis (PCA) on a large set of images depicting different human faces. Informally, Eigenfaces can be considered a set of "standardized face ingredients", derived from statistical analysis of many pictures of faces. Any human face can be considered to be a combination of these standard faces.

The Eigenfaces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern is how different features of a face are singled out to be evaluated and scored. There will be a pattern to evaluate symmetry, if there is any style of facial hair, where the hairline is, or evaluate the size of the nose or mouth. Other Eigenfaces have patterns that are less simple to identify, and the image of the Eigenfaces may look very little like a face.

Linear equations Ax D b comes from steady state problems. Eigenvalues have their greatest importance in dynamic problems. The solution of du=dt D Au is changing with time—growing or decaying or oscillating. We can't find it by elimination.A100 was found by using the eigenvalues of A, not by multiplying 100 matrices. Those eigenvalues (here they are 1 and 1=2) are a new way to see into the heart of a matrix.

To explain eigenvalues, we first explain eigenvectors. Almost all vectors change direction, when they are multiplied by A. certain exceptional vectors x are in the same direction as Ax. Those are the "eigenvectors". Multiply an eigenvector by A, and the

Vector Ax is a number _ times the original x.

The basic equation is Ax D _x. The number _ is an eigenvalue of A.

The eigenvalue _ tells whether the special vector x is stretched or shrunk or reversed or left unchanged—when it is multiplied by A. We may find _ D 2 or 1 2 or _1 or 1. The eigenvalue_ could be zero! Then Ax D 0x means that this eigenvector x is in the null space.

If A is the identity matrix, every vector has Ax D x. All vectors are eigenvectors of I .All eigenvalues "lambda" are _ D 1. This is unusual to say the least. Most 2 by 2 matrices have two eigenvector directions and two eigenvalues.

III. LITREATURE SURVEY

Before working on this idea, we consulted the below research papers:

• [A]: A Robust Skin Color Based Face Detection Algorithm by Sanjay Kr. Singh, D. S. Chauhan, Mayank Vatsa, Richa Singh

• [B]: Fast Face Recognition by Karl B. J. Axnick and Kim C. Ng

•[C]: AN EFFICIENT WAVELET/NEURAL NETWORK-BASED FACE DETECTION ALGORITHM by Bardia Mohabbati, Mohammad Shiri, Shohre Kasaei

• According to [A] a comparison has been made for detecting faces in the controlled background, using skin colour detection on RGB, YCbCr and HIS colour spaces. We have found that YCbCr and his colour space are more efficient in comparison to RGB to classify the skin region. But still both are not able to give very good results.

• Based on the results of the three algorithms, we have combined from this region(s) facial feature (eyes, ear and mouth) has been extracted from a proposed facial feature extraction algorithm which finally gives the detected face. It is robust and efficient in classifying the skin color region and face region. Accuracy of proposed algorithm is 95.18%.

• According to [B] fast face recognition system is quite accurate even though pose, illumination and expression variations were present. The performance with 2D color images was 97% accuracy with one second processing time per face and this system has been tested in real time on live faces for access control successfully. As more scans are added to the system the accuracy will likely fall,

• However the use of locally focused neural networks around the salient feature points (which will be mapped to hardware) is currently being investigated. The 3D method has already achieved 100% accuracy and is readily deployable for use in access control. Unfortunately the current 3D scans require that the subject stay still for 0.4 seconds while an eye safe laser scans them. A more user friendly and more covert stereo vision system is being developed to speed up scanning and improve through put. However as stereo vision will not be as accurate and robust as the laser, a performance decrease might result.

• In contrast, holistic face recognition methods which use entire face images in a 'grab all' manner can easily be corrupted through the pose, illumination and expression variations. Other geometric methods such as local Gabor Wavelet filters would however yield more accurate results than this paper's geometric method.

• Wavelet examination of the local area data around salient points is more detailed and robust (as it tests a lot more points) compared to the heuristic methods. However the increased complexity and running time of such methods may rule them out for access control applications. Also by using the local areas as recognizable features these algorithms are less resistant to expression, shade and pose variations.

• According to [C] multilayer perceptron (MLP) is trained to classify pixels into skin-tone and non-skin-tone. The input vector to the network consists of (Cb,Cr) values corresponding to chrominance. Image database used consists of 240 images of positive and negative training patterns. Also, 150 images containing group photos were collected.

• Skin colors from various races of the world are collected in the form of 32 × 32 pixels per skin sample for each individual from each image. 120 such samples were collected Cb-Cr planes. As a result, there are 122,880 skin pixels

having different illuminations in our skin color database used for training the neural network. The neural networks were trained using Levenberg-Marquardt (LM) method in order to generate binary outputs for skin and non-skin. The Levenberg-Marquardt method will have the fastest convergence compared with other methods such as conjugate gradients or gradient.

• In general, the LM algorithm will have the fastest convergence for networks that contain up to a few hundred weights, like the topology being brought up by the authors of this article. The scalar output of MLP is converted into binary output, 0 as non-skin and 1 as skin, using a fixed threshold = 0.35 and sigmoid as activation function. The MLP classifiers that we trained have one hidden layer ranging from 9 to 25 neurons.

• Furthermore, different network sizes were investigated but we only report the performance of the most efficient network. The best result was 89.6 correct classification achieved with the neural networks of size (2-25-1) (one hidden layer of 25 neurons), and the false detection and false dismissal rate were 4.6% and 4.5% respectively.

• The appropriate skin-colour decision boundary is generated by training neural networks with 1000 to 5000 samples. The algorithm starts at the LL sub-image, a lower resolution version of the image obtained from the wavelet transform, so that the amount of data to be processed is greatly reduced. The lower resolution image is sufficient for the detection of face regions rather than detailed low-level features.

• So, whenever any pair of (Cb,Cr) gets classified as skin pixel, it means that the corresponding area of 16 × 16 pixels with respect to this pair is a face block. After the classification, a binary mask image is obtained for each image but with a reduced resolution.

• Each value in the mask image indicates the classification results of the corresponding block of size 16 × 16 in the original image. A skin and non-skin colour classifier using multilayer perceptron is presented. The major advantage of the new method is that accurate approximation of the decision boundary for skin colours in Cb-Cr planes is achievable with small-sized networks. The neural network based model has been shown to provide remarkable coverage of all human skins.

• The utilized MLP classifier is a good candidate if low memory usage is also a requirement. This also provides a promising direction for the efficiently and accurately extracting skin irrespective of colour of the skin as is evident from the results. One of the most remarkable merits of our proposed algorithm is that, unlike a plethora of others, it attenuates the problem of containing exhaustive searches. The computation time has been reduced considerably. However, it is to be noted that the training neural networks is performed off-line.

• Hence, neural networks computational cost is not substantial, and computation time needed to calculate is the forward wavelet transform of the image in real-time processing. By adjusting the thresholds in all stages, face detection rate can be controlled depending upon the application. Nevertheless, it is not entirely full-blown and suffers from a couple of shortcomings and cannot be taken into account as generalized. Moreover, it can only be applied to colour images, because of the use of chrominance information. The algorithm gives false alarms under non-uniform lighting conditions which is seemingly inevitable in such algorithms. False dismissals cannot be totally avoided, especially in a very cluttered scenes with many small faces.

• In the final analysis, despite its restrictions, the proposed face detection is efficient and can be applied to large image databases for indexing and recognition. Once these face regions are detected, they can be further used for face tracking, and face recognition using more sophisticated techniques. Further work is in progress to develop a real-time face tracking and recognition system and index individuals for surveillance purposes.

IV. OBJECTIVE

Through this application, we propose to take the database security measures to the next level. Amongst the various measures which are adopted to secure the data records, we have planned to implement the concept of identifying and authenticating the physical features of humans which access the data. In other words, we validate and restrict the access to the database according to the roles assigned to human beings for records accessibility, the basis of their facial features.

As we know, the data is accessed and managed through functions which apply various calculative actions on the records. For ex: Data can be manipulated through, insertion of fresh data, modification of existing data or deletion. In order to assign these functions, we need to create roles for the users who may access these functions via the roles assigned to them and through this application, we propose to assign and authenticate these roles through the recognition of facial data.

We know that the relevance of data security is in all the business verticals like Banking, Retail, Manufacturing, Hospitality, etc. Hence, we have chosen banking domain which holds critical and sensitive client data that is accessed and managed everyday by its employees. Through this application, we shall register the new employees within the bank not only by assigning a User ID & Password but also through capturing and registering their facial data information in the database.

In other words, when a new employee is recruited by the bank, the Administrator shall register that employee by inputting his / her personal details along with the facial data wherein the employee will have to get his / her face captured in front of a camera in real time after only which the user id and password shall be generated.

One important aspect of the registration feature is, during this process, the Administrator shall also assign the roles or responsibilities to the employee. In this application, we have assumed that 4 roles could be assigned to any employee i.e. Create Customer, Edit Customer, Lock Account and Unlock Account.

As the name suggests, creation of customer will involve opening of fresh bank accounts. Editing shall involve the modification of existing customer data that hold accounts in the bank. Lock account will lock the account of a customer

after which he / she will not be able to make any further transactions and Unlock account will unlock the locked account of a customer. Lock account will be used in the scenario when the customer requests for locking his bank account in the possible event of loss of debit or credit card.

As these roles involve different levels of modification and accessibility to the customer data of the bank, it becomes extremely essential that we assign these roles carefully to the employees according to any specific criteria and also ensure that when a user accesses the roles, he/she must be thoroughly validated for same for authenticity.

Therefore, we plan that once the user is successfully registered, the appropriate roles will be assigned to him / her and in order to access those roles, the user shall have to clear 2 levels of authenticity checks. First, the user will be required to input the correct user id and password of his / her account. After that is successfully validated, he / she will be authenticated on the basis of his / her facial data which was stored in the database during registration. Hence, immediately after the user id and password are positively validated, the integrated camera of the PC / Laptop will turn ON which will capture the user's face live for few seconds and compare it with the already stored facial data matching to the inputted user id and password.

Only after the user's face is validated and human authentication is properly done, will the user be allowed to log in to the system and access his / her roles which will grant him the access of managing the customer records / data of the bank according to the assigned roles. In this way the records of the database will be secured from an unauthorized access because human (physical) verification will come into play. So, even if the user id and password of an employee is compromised, there would be no possibility that the human verification be bypassed.

V. PROBLEM STATEMENT

We identified the existing problems as below:

1) There is a bank that has a lot of customers. The bank wants to protect the data of its customers so that it cannot be accessed illegally.

2) The bank wishes to maintain the integrity of the data so that if a request arises for the access or retrieval of the data along with its modification, the bank is able to control it.

3) The bank wishes to assign or categorize employees who can have the privilege to access or modify the data. It wants to categorize the employees based upon their experience and skills.

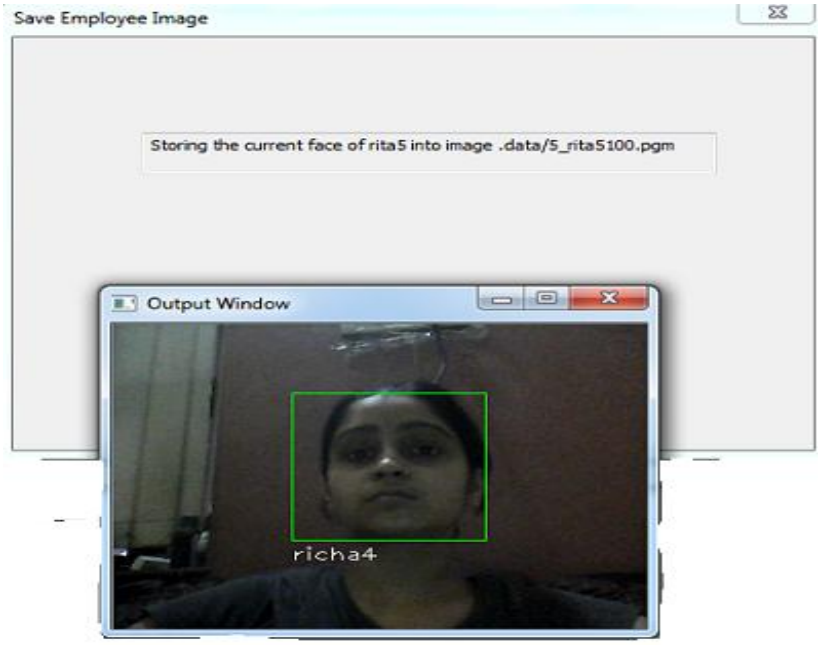
4) The security measures are not sufficient in order to protect the customer's data. The bank wants to fortify the data protection by applying multi – level encryption techniques.

5) There is a need to check whether an employee is physically present on his / her system while working on the customer's records in order to access or modify it. Because the user id and password of any employee can be easily compromised the bank wishes to check whether the employee is physically present on his / her desk.

VI. PROPOSED SOLUTION

 when a new employee is recruited by the bank, the Administrator shall register that employee by inputting his / her personal details along with the facial data wherein the employee will have to get his / her face captured in front of a camera in real time after only which the user id and password shall be generated.

 one important aspect of the registration feature is, during this process, the Administrator shall also assign the roles or responsibilities to the employee. In this application, we have assumed that 4 roles could be assigned to any employee i.e. Create Customer, Edit Customer, Lock Account and Unlock Account. Pages other than the first page, start at the top of the page, and continue in double-column format. The two columns on the last page should be as close to equal length as possible.



VII. RESULTS

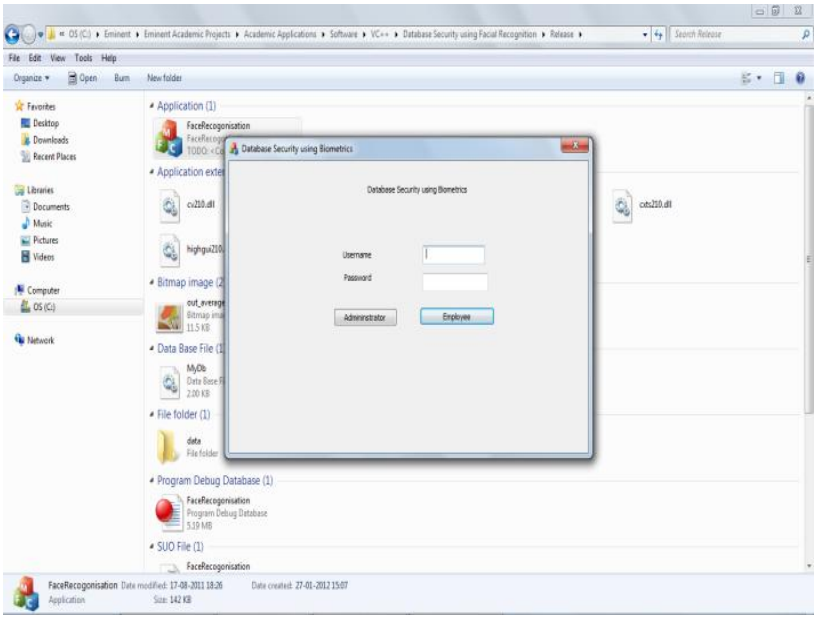


Fig 1. Administrator or employee login page

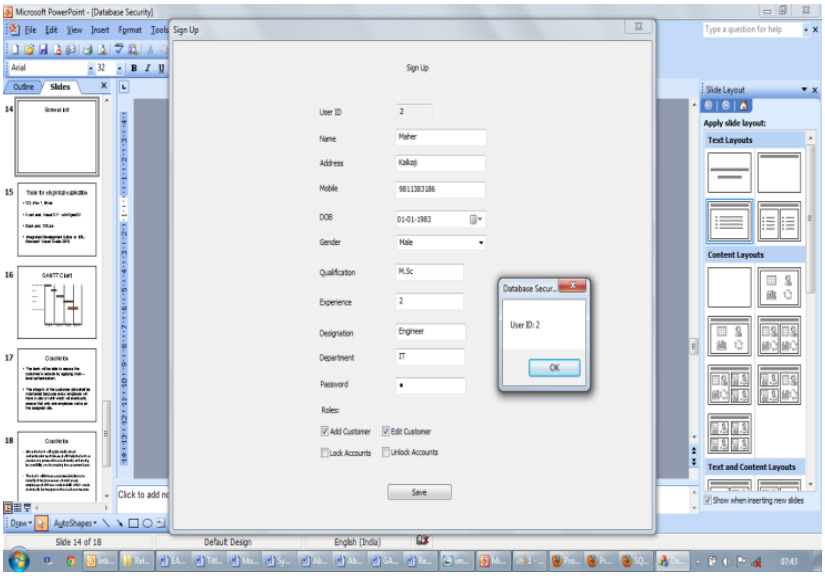


Fig 2. Employee registration

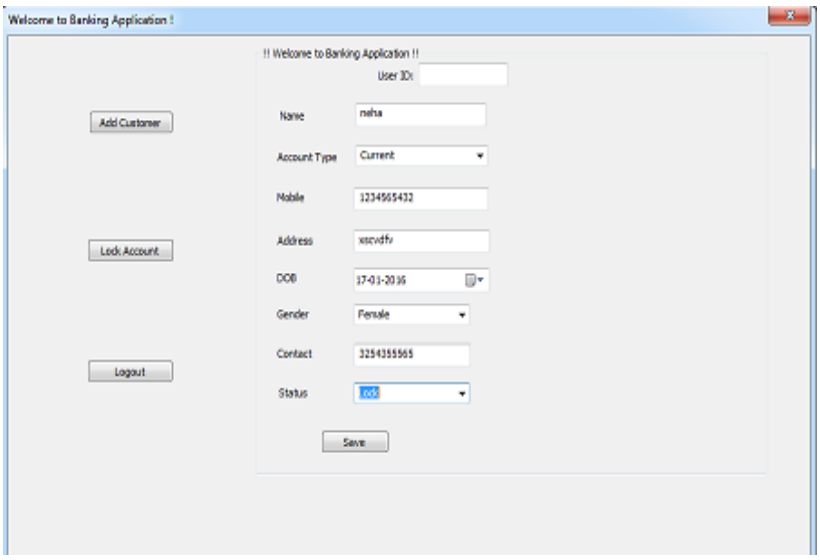


Fig 3. Customer registration

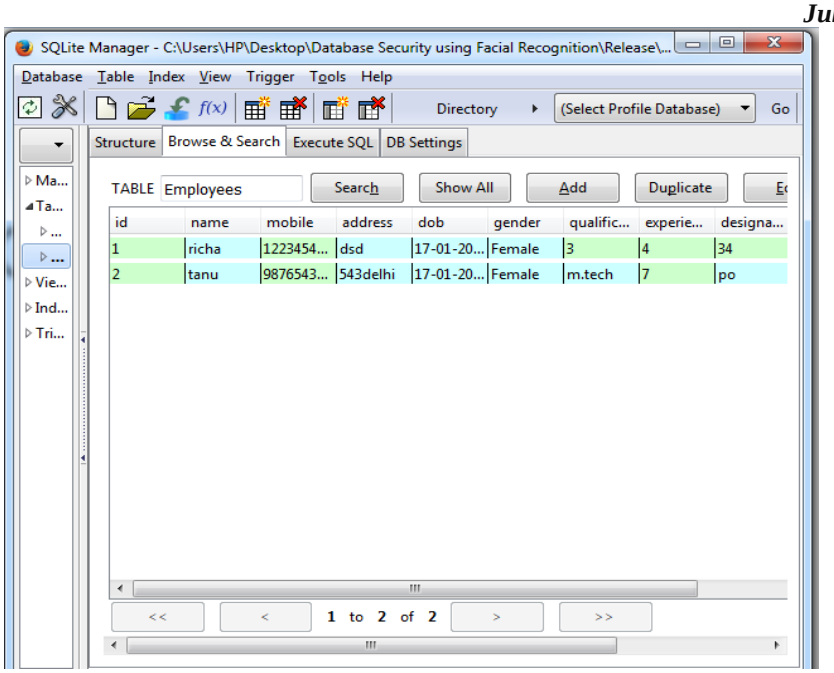


Fig 4. Employee records

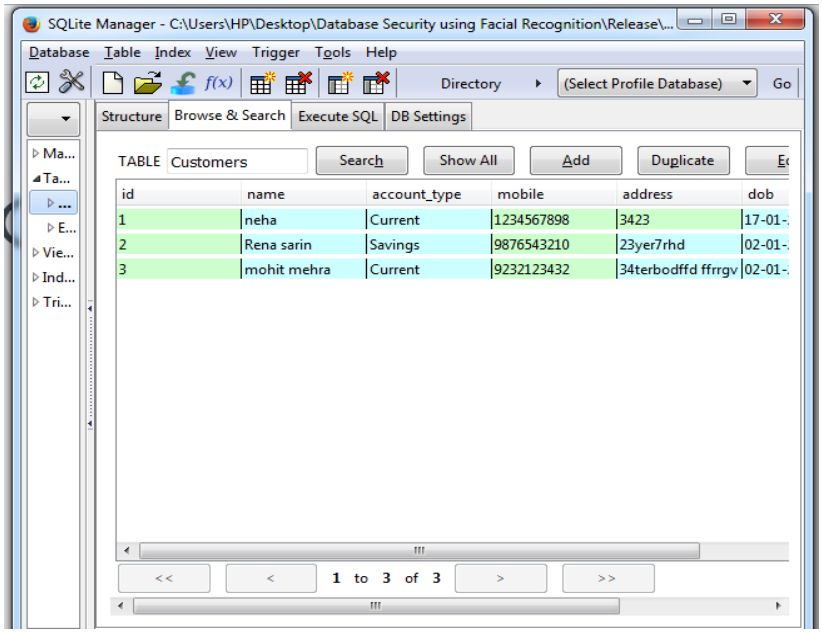


Fig 5. Customers records

VIII. RESEARCH METHODOLOGY

The research methodology which we have followed in our thesis is of type Exploratory. Before formulating this idea, we explored and studied about the domains like Database, Database Security and Human Authentication methodologies. We explored about the prevalent issues in the domains of database security and how they can be more effectively solved using advanced techniques that may involve a hybrid implementation of database security along with the concepts of human verification.

Then, we explored and studied about the existing techniques which are used for the purpose of securing the records. During our research, we found that the security mechanisms are generally role-based in which the users are assigned some specific roles using which they can access the database records. Hence, we planned to inflate and extend our research beyond measures through which the databases can be secured by applying multi-layered security procedures through which the enforcement of verification and authentication is not just only at the user level but should also be at the role-level which is used to access or modify the records. Thus, in our research, we proposed to develop a strategy which combines role mapping along with human verification in order to secure the database.

IX. CONCLUSIONS

Keeping this application into context, we can safely conclude that. It can be effectively used in all the business verticals where secured access of database records is a necessity. This application combines the power of database role-mapping with human verification for the security of records. Through this application, not only the records will be

secured but data definition and manipulation procedures will also be effectively enforced. This application will effectively allow the new users to safely access the data through minimal roles assigned to them which can be duly changed at any point of time in future.

During the second layer of multi-layered security mechanism which is human authentication, this application shall not allow the user to keep his/her face before the camera for a long time. There is a time-based human verification which will be implemented and this new concept shall surely strengthen the security during accessibility of the database records.

ACKNOWLEDGMENT

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template.

REFERENCES

[1] A Robust Skin Color Based Face Detection Algorithm by Sanjay Kr. Singh, D. S. Chauhan, Mayank Vatsa, Richa Singh
[2] Fast Face Recognition by Karl B. J. Axnick and Kim C. Ng
[3] AN EFFICIENT WAVELET/NEURAL NETWORK-BASED FACE DETECTION ALGORITHM by Bardia Mohabbati, Mohammad Shiri, Shohre Kasaei
[4] Fundamental of digital image processing by Jain Anil k
[5] Digital Image Processing by Rafael e González
[6] Dudgeon, D.E. and R.M. Mersereau, Multidimensional Digital Signal Processing. 1984, Englewood Cliffs, New Jersey: Prentice- Hall.
[7] Castleman, K.R., Digital Image Processing. Second ed. 1996, Englewood Cliffs, New Jersey: Prentice-Hall.
[8] Oppenheim, A.V., A.S. Willsky, and I.T. Young, Systems and Signals. 1983, Englewood Cliffs, New Jersey: Prentice-Hall.

