Unique Identification System

Alankrit Patnaik
Bhagwan Parshuram Institute of Technology
Delhi, India

Deepak Gupta
Bhagwan Parshuram Institute of Technology
Delhi, India

ABSTRACT

Unique Identification System is a system in which every citizen of a country will have a unique 16 digit number Unique Identification Number which would not just help the government track down individuals, but would make life far easier for citizens as they would not have to submit multiple documents each time they want to avail a new service—public private, government., regulatory authority or law-enforcement agency. This system will contain details like the name, sex, address, marital status, photo, identification mark and face biometrics. The unique identification number will be based on a sophisticated application called SCOSTA, a secured electronic device that's used for keeping data & other info in a way that only authorized persons can view it. The security of the UID database system will be handled by the Biometric technology. The system would provide a database of residents containing very simple data in biometric. The UID system's database is built by collecting data from different existing databases distributed all over the country, combining and storing it in one centralized UID system database helping to develop a card which can be centrally issued and used everywhere. This document tells us about the benefits and capabilities that will be provided to the identification system. It also states the various requirements, specifications, advantages and constraints that the system should abide by. UID system helps in managing a single number for every person needs in his/her life span i.e. the number is used as Driving license number, Voter ID card number, registration number in any organization, bank account number, personal or professional details. Security mechanism in UID one wonders - if there is no physical Identity card or electronic smart card, then how will UID validate its citizens. For implementing this, two different processes have to followed, the first one being the recording process and the second one - the authentication process. The UID is fundamentally prepared to identify citizens so that better security can be provided by identifying illegal immigrants and terrorists. The role the system envisions is to issue a unique identification number (UID) that can be verified and authenticated in an online, cost-effective manner, and that is robust enough to eliminate duplicate and fake identities.

Index Terms *— Unique Identification System, Face Recognition System, Role based Access Control, SCOSTA, SQL, DRP, ETDC, STQC, RBAC.*

I. INTRODUCTION

The purpose of a Unique Identification System is that it avails a Unique Identity Number to the citizen of a country giving them the advantage of not submitting multiple documents to avail the services residents would no longer need to go to various government departments and prove their identity each time. This scheme is designed to leverage intensive usage of the UID for multipurpose to provide an efficient and convenient mechanism to update information. Photographs and biometric data are added to make the identification and authentication foolproof. The unique ID will require creation of a database that links an individual to unique identifier formed, based on a format code that remains constant over his life-span, like parentage, date and place of birth and automatically gets activated just like a voter ID card. The UID database is built by collecting data, storing and linking the existing Identity databases (voter ID, passports, ration cards, licenses, fishing permits, border area ID cards) into one centralized database from which the information can be accessed. The UID Authority will be responsible for creating and maintaining the core database and to lay down all necessary procedures for issuance and usage of UID including arrangements for collection, validation and authentication of information, proper security of data, rules for sharing and access to information, safeguards to ensure adequate protection of privacy. Data association at present with UID, are the following 13 parameters. a. Name b. UID Number of the holder c. Photograph d. Right hand forefinger print e. Name of the Father f. Name of the Mother g. UID of the Father h. UID of Mother i. Date of Birth j. Sex k. Place of Birth l. Blood Group m. Address at time of creation

It is necessary to consider if all of them need to be considered as a primary ID parameters or can be classified further as "Primary" and "Secondary". The UID will be a Root ID for downstream services available to the Citizen so that there is a need to recognize one single "Root UID Parameter" so that in the event of any dispute, the UID would be owned by the person in undisputable control of the "Root ID Parameter". The reason of segregating the ID data into "Primary" and "Secondary" is that some of the ID parameters can be kept out of the Primary data base and can even be kept offline. While the primary database has to be accessible on the Internet and despite the authentication mechanisms used or Disaster Recovery Plan (DRP) strategies, they are still amenable to hacking attacks. The secondary data base however can be kept away from the Internet and in multiple formats so that the data in the secondary data base can be used for verification when the primary data is disputed. For example, we may collect multiple biometric features say 1. Left hand thumb print scan 2. fingers scan 3. geometry scans.

In the current scenario, each of the ID parameters are classified as "Primary" and "Secondary" in context of database storage:

1.1 FORMAT OF UID CODE NUMBER-

<u>NAME:</u> Primary Database- Initials; Secondary Database- Expansion of Initials, Father, Grandfather.
<u>UID NO. of Holder:</u> Primary Database
<u>PHOTOGRAPH:</u> Primary Db- Date of Issue of UID as reference
<u>Right Hand Fore fingerprint:</u> Primary ID Db; Sec. Db- Rest 9 fingers
<u>NAME OF FATHER</u>
<u>NAME OF MOTHER</u>
<u>UID OF FATHER:</u> Primary Database
<u>UID OF FATHER</u>: Primary Database
<u>DATE OF BIRTH</u>: Primary Db; Sec. Db- Time of Birth
<u>SEX:</u> Primary Database

PLACE OF BIRTH: Secondary Database
BLOOD GROUP: Secondary Database
ADDRESS AT TIME OF CREATION: Secondary Database

1.2 DESIGN AND FEATURES OF UID CARD

The UID card will be with 64KB of memory designed to be in line with the specifications laid out in ISO/IEC 7816 and SCOSTA.

The cards are designed to support a minimum of 300,000 EEPROM write cycles and will retain data for at least 10 years.

The identity card being given to each individual citizen has a microprocessor chip with a memory of 64 KB which is enough space to accommodate all service links and makes it secure.

Besides having several physical features into the design of the card, it is the cyber security using 'asymmetric key cryptography' and 'symmetric key cryptography' that has made the card secure against the risk of tempering, cloning and hacking as well.

This study considers theoretical aspects as well as simulations performed on software developed.

1.3 Organization of paper

The rest of this paper is structured as follows: Section II summarizes the complete details design of the new approach, their algorithms. Section III shows the implementation issues, section IV provides the solution and some security measures. Section V shows some advantages of the proposed system. Section VI gives the basic implementation requirements and finally the paper concludes in Section VII.

II. DESIGN AND ARCHITECTURE

In this section, we describe the Algorithm, which is used to explain how the system is going to work, i.e. the process logic behind it, the flowchart, which represents the pictorial representation of the process logic and finally the Data Flow Diagram (Context Level) of the UID system.

2.1 ALGORITHM

Security mechanism in UID project - if there is no physical Identity card or electronic smart card, then how will UID system validate its citizens. For implementing this, two different processes have to followed, the first one being the recording process and the second one - the authentication process.

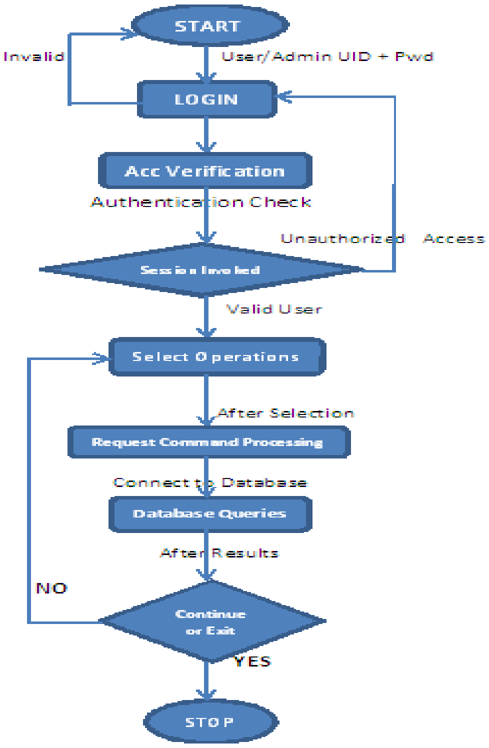
RECORDING PROCESS: In the first process, the UIDAI builds up a centralized database consisting of UID, biometric record and various other details of the person. The UIDAI allocates a unique 16 digit number (UID) which is randomly generated by the main computer to every citizen. Then a biometric data record is made by scanning the iris or 10 fingerprints of a person. This biometric data is tagged to the person's unique 16 digit number (UID). The UID tagged to the biometric record of a citizen is later used in the authentication process.

AUTHENTICATION PROCESS: In the second process, whenever a person has be identified whether he/she is a genuine one, a fresh biometric scan is made and then the scanned image is sent to the centralized server. The server takes the fresh scanned biometric image as an input and compares it with all the already stored biometric records in the database. If a relevant match found is found, then the person is designated to be a genuine citizen.

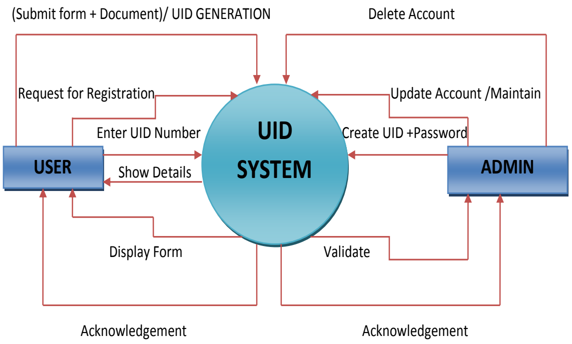
BASIC STEPS FOLLOWED:

1	The basic process of UID follows as if the user is already registered with UID system, then he/she simply enters his/her UID No. & logins to view his/her account details. The user is restricted to Update/delete or create any account.
2	But if the user is new to UID system, he/she has to first fill the key form manually regarding all the information of his/her respective different fields and submit it to registrar to be at a later stage. This stage is an internal process and will not be shown anywhere in the Interface.
3	Next after the verification by the online registration the data form is given to the admin. Admin generates or allots a UID no for the user who register validate and acknowledges.
4	a)The Admin has its own registration no., and a password so that no other person can access it (for security reasons) b) Admin has a database of its own so as to store his/her details as well. c) After login the Admin has four options: Create View, Delete, and Update.
5	Creation step: In creating account the UID allotted is entered details are added and submitted to the database with the help of a submit button in the interface.
6	Update/Delete step: In updating account the UID allotted is entered details are updated/deleted and submitted to the database with the help of an Ok/Delete button in the interface along with an acknowledgement.
7	The user account, say after creation/updating/deletion is acknowledged and the user is made aware of it.
8	The format of the UID number or the UID is generated on a pattern which looks like this: Name Father's name DOB Blood group.
9	The Internal process of this is that the user details are fetched from a database with UID No. acting as a primary key in all respective table as an attribute and also act as a foreign key in other table
10	To fetch details of admin, admin has its own database when required fetches data from database and displays it to admin

2.2 FLOW CHART



2.3 DATA FLOW DIAGRAM



III. IMPLEMENTATION ISSUES/PROBLEMS

3.1 ONLINE AUTHENTICATION

Authentication by taking a fingerprint of a person and sending it across a mobile phone and establishing identity has many challenges. The scanned fingerprint image is sent to the centralized database server by the person, the online authentication is done by a "Yes" or "No" response along with name/age/address. In this process, one of the key issues is to ensure that the scanned fingerprint image to be sent is a secured line i.e. all communications are encrypted and then sent to the other terminal, otherwise the outbound signal of fingerprint data can be manipulated by a hacker. Hence if incorrect data is given to the central database, the response from the authentication process would also be incorrect.

3.2 BIOMETRIC

Electronic scanning and matching technologies are not 100 percent error-free. Since biometrics is not an exact science, the problem is not only is the underlying data flawed, even the biometric technologies have some error rates. Given the large numbers involved, even a 5 percent error rate will translate into 50 million records being matched incorrectly. At the time of purchasing biometric scanning equipments, it is important to include a clause mentioning the calibration requirements. Once the biometric scanning equipments are purchased, UID authorities should also collaborate with the Government based Electronics Test & Development Centre (ETDC), Standardization, Testing and Quality Certification (STQC) to ensure that the purchased biometric scanning equipments are free of errors.

Scanning - Practical Challenges

While biometric data in digital format is the norm for modern day authentication process, choosing the right type of scanning device is more important. While fingerprinting is the most straightforward biometric available, iris scans are more reliable. But the equipment for iris scans is expensive and the implementation process is cumbersome. The erosion of fingerprints of people who are involved in heavy physical labour or eyesight being affected over a period of time is one such challenge. In case of eye scan, eye sights or surgery or accident can make the biometrics non-usable. In such instances, experts are of the view that UID authority may take all 10 fingerprints.

3.3 PRIVACY ISSUES

Privacy is a key concern as all of an individual's personal (biometric) information will be stored in one database where the possibility of corruption and exploitation of data is far greater than when having the information disbursed. Risks that arise from this centralization include possible errors in the collection of information, recording of inaccurate data, corruption of data from anonymous sources, and unauthorized access to or disclosure of personal information. The UID authority has to strike a balance between "privacy and purpose" on the biometric data collected from the citizens. The biometric database of people should not be misused in any way by the personnel of UID authority or others. Suppose the biometric data (digital fingerprint) of a person is compromised, then the consequences of such incidents are fatal because the digital fingerprint is basically used for authentication process. Hence if the critical biometric data of a citizen is compromised, all future authentication process for such person could prove wrong. So, UID must be secure from malicious elements - both internal and external sources.

3.4 RESPONSIBILITY FOR DATA SECURITY

In view of the criticality of the UID operation, the "Reasonable" security *practices* may have to be substantially stringent. It is necessary to implement globally acceptable principles of data security and privacy protection to meet the requirements.

Some of the specific requirements which can be implemented under this framework for ITA 2008 compliance include

1. Obtaining the consent of the UID holders for inclusion of the data which would be in the form of an application made by the data subject and validated in its electronic form.

***** If data is validated on paper and the UIDAI takes the responsibility for digitization then some member of UIDAI should be held accountable for any inaccurate data that may creep in. Such a person has to validate the electronic form of the data with his digital signature and take the legal liability for the inaccuracies.

***** A copy of the data as entered in the data base has to be provided to the data subject in print form with appropriate certification under Section 65B of Indian Evidence Act as per established principles of Cyber Evidence Archival.

***** As a part of this data validation process, it may be necessary to provide access to the data in the data base to the holder of the UID so that he can verify the data any time and any number of times during the lifetime of the data.

***** Though this facility may not be used by many of the UID holders who are not cyber savvy, it is an essential part of Cyber Law Compliance.

***** This may require validation of the person making the query. If we need to use "Digital Signatures" for validation, the UID itself may have to also include an "e-mail address" in the minimum as a "Digital Identity parameter".

2. Data has to be encrypted in storage and every element of the data base has to be digitally signed by an officer of the UID.

3. Appropriate audit trail of who accessed the data and what was the hash value of the data accessed before and after the access session etc will have to be captured along with the mode of access, IP address etc and archived in such a manner that they are available for judicial scrutiny when required.

4. The hardware and software used by UID authority should be source code audited and certified for integrity. Supplies from countries suspected to be preparing for Cyber Warfare against a particular country must be avoided.

IV. SOLUTION/SECURITY MEASURES

Availability of stored data in the database being accessed online through leased or dedicated networks is subjected to hacks from hackers through any nodal points. To address this, an effective control on the data being accessed is required. Role Based Access Control (RBAC) based model would be an ideal choice for centralized UID system. To be specific, sensitive information in the UID database like biometric data has to be accessed by authorized personnel only and not by any other persons who do not have the specific access rights.

Role-based access control (RBAC) is an approach to restricting system access to authorized users. It is a newer alternative approach to mandatory access control (MAC) and discretionary access control (DAC). RBAC is sometimes referred to as role-based security. Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user; this simplifies common operations, such as adding a user, or changing a user's department.

Three primary rules are defined for RBAC:
1. Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a role.
2. Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
3. Transaction authorization: A subject can execute a transaction only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.
Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles.

When defining an RBAC model, the following conventions are useful:

- S = Subject = A person or automated agent
- R = Role = Job function or title which defines an authority level
- P = Permissions = An approval of a mode of access to a resource
- SE = Session = A mapping involving S, R and/or P
- SA = Subject Assignment
- PA = Permission Assignment
- RH = Partially ordered role Hierarchy. RH can also be written: ≥ (The notation: $x \geq y$ means that x inherits the permissions of y.)
- A subject can have multiple roles.
- A role can have multiple subjects.
- A role can have many permissions.
- A permission can be assigned to many roles.

A constraint places a restrictive rule on the potential inheritance of permissions from opposing roles, thus it can be used to achieve appropriate separation of duties. For example, the same person should not be allowed to both create a login account and to authorize the account creation.
Thus, using set theory notation:

- $PA \subseteq P \times R$ and is a many to many permission to role assignment relation.
- $SA \subseteq S \times R$and is a many to many subject to role assignment relation.
- $RH \subseteq R \times R$

A subject may have multiple simultaneous sessions with different permissions.

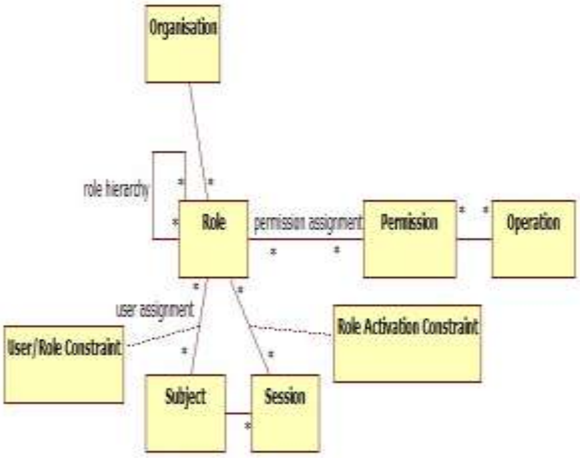


Fig 4.1 COLLABORATION DIAGRAM

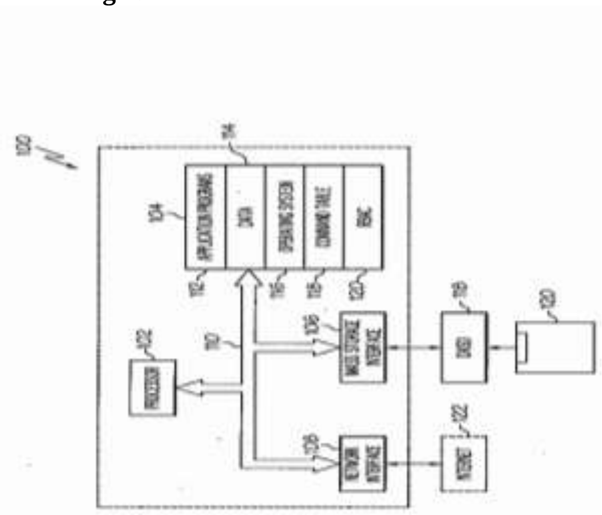


Fig 4.2 ARCHITECHTURE OF RBAC MODEL

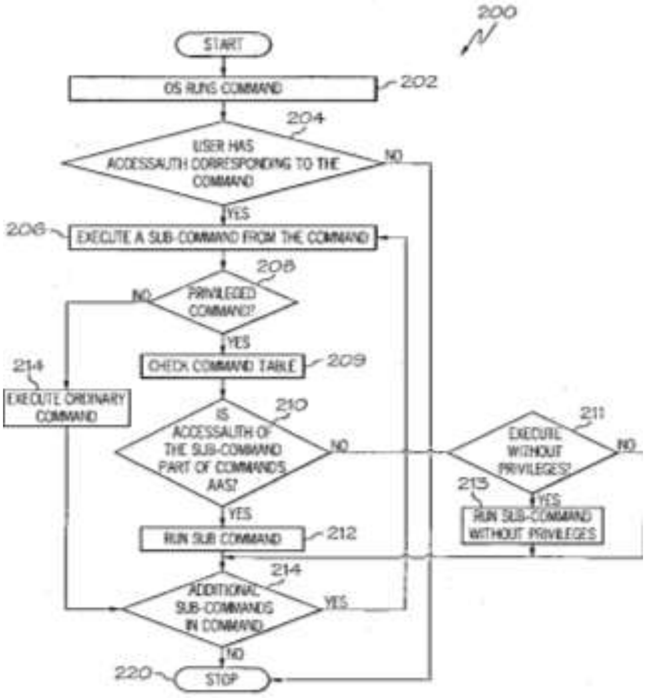

200
START
OS RUNS COMMAND
202
204
USER HAS ACCESSAUTH CORRESPONDING TO THE COMMAND
NO
YES
206
EXECUTE A SUB-COMMAND FROM THE COMMAND
208
PRIVILEGED COMMAND?
NO
YES
CHECK COMMAND TABLE
209
214
EXECUTE ORDINARY COMMAND
210
IS ACCESSAUTH OF THE SUB-COMMAND PART OF COMMAND'S AAS?
NO
211
EXECUTE WITHOUT PRIVILEGES?
NO
YES
215
RUN SUB-COMMAND WITHOUT PRIVILEGES
YES
RUN SUB COMMAND
212
214
ADDITIONAL SUB-COMMANDS IN COMMAND
YES
NO
220
STOP

Fig 4.3 FLOW CHART FOR RBAC

V. ADVANTAGES

- Define mechanisms and processes for interlinking UID with partner.
- Databases on a continuous basis.
- Frame policies and administrative procedures related to updation.
- Mechanism and maintenance of UID database on an ongoing basis.
- Define usage and applicability of UID for delivery of various services.
- Evolve strategy for awareness and communication of UID and its usage.
- Issue necessary instructions to agencies that undertake creation of Databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner databases.
- Manage all the details related to the Bank account, Driving License, Vehicle registration, Voter ID card, Medical records, education and profession, passport, PAN card in one database. A single unique number is used therefore decreasing manual labour and increasing efficiency as every detail is available on the single click and reducing the efforts in maintaining different ID databases. The UID will reduce d duplication, an attempt to make fake documents.

- The purpose of this UID system is to provide one unique number to all the citizens to increase the security and verification process by introducing the Biometric authentication technology, and thus identifying illegal immigrants and terrorists.

VI. IMPLEMENTATION REQUIREMENTS

6.1 DEVELOPMENT ENVIRONMENT

I had also developed softwares based on our study on “UID System” and “Face Recognition system” which includes the simulation of the prototype, as how will the process logic is implemented in practical conditions, the fundamental properties of the real time face recognition software, which was developed to demonstrate the proposed real time face recognition approach for biometric security purpose.

6.1.1 System/ Hardware Requirements

It is an MS Windows based application. Minimum hardware and operating system requirements in order to run this software efficiently are given below:

○ *Operating System:* Windows 98/ME/2000/XP,

○ *RAM:* 64MB,

○ *Video Adapter:* should be compatible with DirectX

○ *Digital camera/Web camera* with resolution 320x240(R, G, B), 15fps

○ *Primary Database storage:* for storing the primary ID data

○ *Secondary storage:* for storing the face image database and secondary ID data

6.1.2 Software Requirements

Microsoft SQL Server 2005 or Oracle 9i.

Visual Studio.NET 2008- C# language is required to create the source code. It is this language which will form the support of the system.

Operating System**:** Windows 98/ME/2000/XP

6.1.3 Performance requirements

1 Static Numerical Requirements:

a) Number of Terminals Supported: Numeric
b) Number of simultaneous users supported: ONE
c) Amount and type of information handled: Alpha Numeric, Numeric, Character, Special Symbol

2 Dynamic Numerical Requirements:
a) Number of Transactions: ONE
b) Amount of data to be processed in a timeframe: Alpha Numeric

6.2 SNAPSHOTS

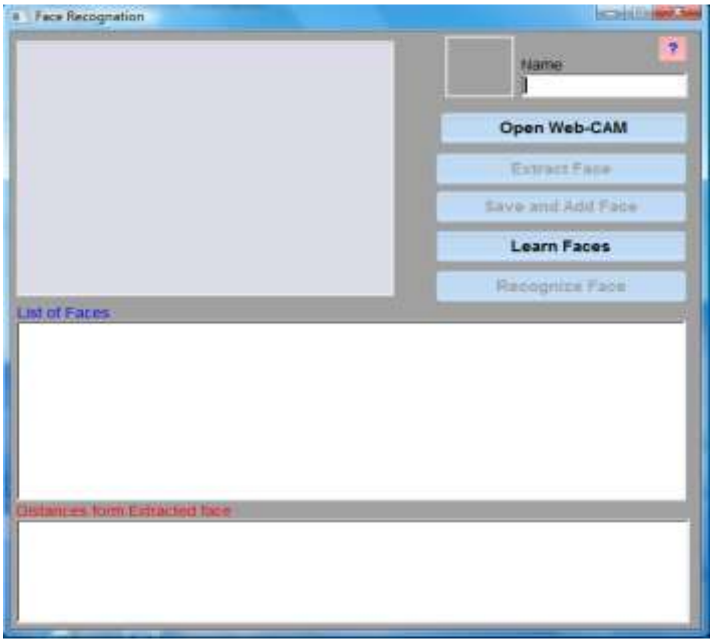


Fig 6.1

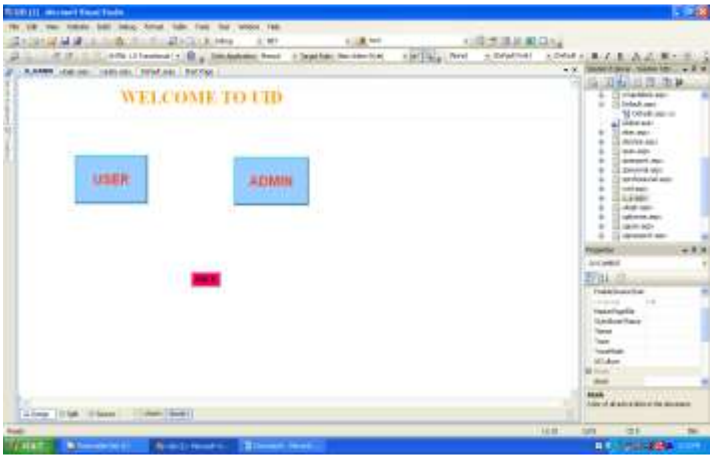


Fig 6.2

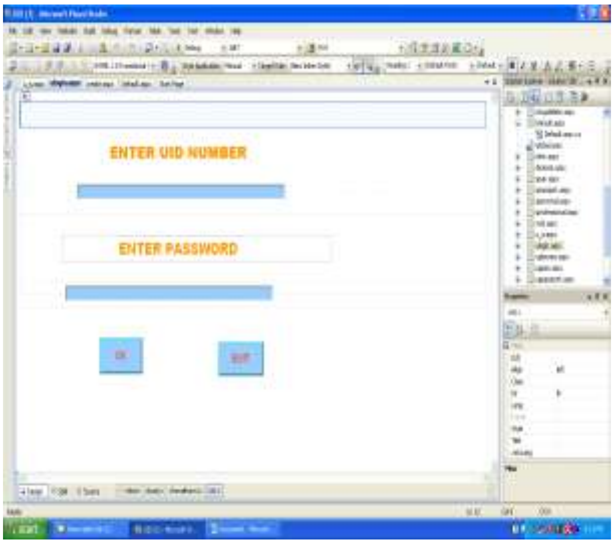


Fig 6.3

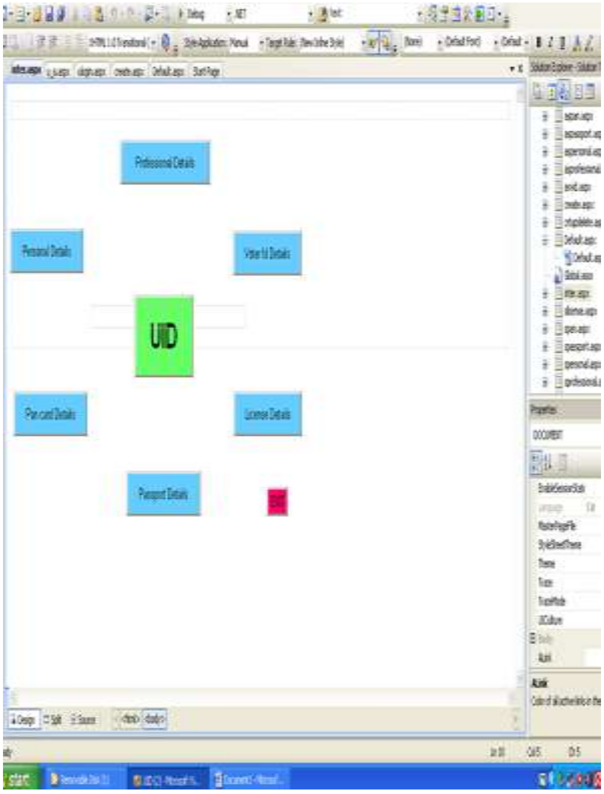


Fig 6.4

VII. Conclusion

Unique Identification System will be beneficiary to the citizens as it is a unique number which contains basic information of every person. After the ID will be issued there is no need to carry driving license, voter cards, pan card, etc for any govt. or private work. For example, for opening a new account one has to show his/her Unique ID only. But to some extent it is harmful to the general public as all the data related to them is stored on computers and can be misused by hackers if the multiple security strategies will not be adopted.

The UID authority in specific should make sure that we have the highest standards of integrity, openness, transparency and process in all stages of UID System.

Implementing and maintaining the UID system will generate high costs along with risks to safety, security, privacy, freedom, and liberty. The UID project should not become compulsory until there is an established judicial overview to ensure that the privacy rights of citizens are not unlawfully violated.

The role the system envisions is to issue a unique identification number (UID) that can be verified and authenticated in an online, cost-effective manner, and that is robust enough to eliminate duplicate and fake identities.

ACKNOWLEDGMENTS

My thanks to my mentor Mr. Deepak Gupta who has contributed towards development of this Research Paper on Unique Identification System

References

[1] “ID'ing the masses may solve Indian identity crisis", *Associated Press*, 17 July 2009.

[2] "India Undertakes Ambitious ID Card Plan", *The New York Times*, 26 June 2009.

[3] “National ID card project", *Indiatimes Infotech*, 1 July 2009.

[4] "Nilekani first chief of Unique ‘ID’ project", *The Assam Tribune*, 25 June 2009.

[5] “Nilekani may get EPFO database for UID project", *Indian Express*, 18 July 2009.

[6] public.ccsds.org/publications/archive/A31x0g1.pdf

[7] "Rs.100 crore for Unique Identification Project", *The Hindu*, 17 February 2009.

[8] securescanbiometrics.com/reference.php

[9] www.answers.com/ident-automated-biometric-identification-system.

[10] www.biometrics.gov/Standards/IXM_Spec_3_1.pdf[10]

[11] www.doi.org/overview/070710-Overview.pdf

[12] www.dtic.mil/whs/directives/corres/pdf/832004p.pdf.

[13] www.ebu.ch/CMSimages/fr/tec_text_d92-2001_tcm7-4721.pdf.

[14] www.faqs.org/patents/app/20090146780.

[15] www.forensicfocus.com/unique-file-identification-nsrl-1.

[16] www.freshpatents.com/-dt20090611ptan20090146780.php

[17] www.hq.nato.int/docu/stanag/auidp/auidp-1-e.pdf.

[18] www.istl.org/09-fall/tips.html

[19] www.morpho.com/spip.php?article1167

[20] www.optoiq.com/.../laser-marking-for-unique-identification.html

[21] www.plos.org/cms/node/133.

[22] www.revenue.ie/en/customs/ecustoms/eori-aeo.html.

[23] www.sersc.org/journals/IJBSBT/vol1_no1/6.pdf

[24] www.uidforum.com/downloads/Atlanta07Presentations/9-11-200-IUID101BasicsDAU.pdf.