Smart Passport System Discrimination Prevention and Crime Detection in Digital Passport System

Pushkar Aswale[1] Bhagyashree Borade[2] Siddharth Bhojwani[3] Niraj Gojamgunde[4]
Prof.Mrs.Bhagyashree Alhat[5]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]MIT Academy of engineering Alandi(D), Pune

Abstract— Data mining is an important technology for extraction of useful data and knowledge that is being hidden in large collections of data. Discrimination comprises of treating people unfairly on the basis of their belonging to a specific group which leads to Crime. Automated collection of data and data mining proficiencies such as classification rule mining have coated the way to make automatic decisions, like passport system, premium insurance computation etc. If the training sets of the data are biased in regards of discriminatory attributes like religion, race, caste, age, etc. discriminatory decisions may take place. For this reason, anti-discrimination techniques including discrimination discovery and prevention have been introduced in online passport system as an application. Online passport is the digital version of the paper passport to provide stronger identity authentication. Since issuing passport is a time consuming process there is a need to lessen amount of human errors and protect against manipulation of travel documents to improve security of system. The proposed system simplifies this process with online portal where the unique identification number is stored which corresponds to the information of the person. This system uses web application technology that uses wireless communication for identification purposes which improves the quality of data and helps to reduce Crime.
Key words: Discrimination; Information Systems; Database Management; Database Applications; Database Security ;Database Integrity ;Protection

I. INTRODUCTION

Advancements in technology have created the possibility of greater assurance of proper travel document ownership, but some concerns regarding security and effectiveness remain unaddressed. The use of online Passport for identification has the potential to make the lives easier, and the world people live in a safer place. The purpose of online passports is to prevent the illegal entry of traveler into a specific country and limit the use of counterfeit documents by more accurate identification of an individual[4]. This online portal focuses on privacy and personal security of bearers of online-passports. Researcher analyzed its main SQL injection features; we focused on vulnerabilities since anyone willing to bypass the system would choose the same approach. On the contrary, solely relying on them may pose a risk that did not exist with previous passports and border controls. The portal also provides a security analysis of the online-passport using User login, Admin login and web application and database[7]. To strengthen border security by reducing forgery and establishing without doubt the identity of the documents bearer[3]. Online passport is measurable characteristics of an individual used to identify him or her. Online systems can function in verification or identification modes depending on their intended use.

II. LITERATURE SURVEY

We have examined how discrimination could impact on cyber security applications, especially SQL injection. SQL injection is in data-driven applications, in which malicious statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). It is obvious that the training data of these systems could be discriminatory, which would cause them to make discriminatory decisions when predicting intrusion or, more generally, crime. Our contribution concentrates on producing training data which are free or nearly free from discrimination while preserving their usefulness to detect real intrusion or crime[9]. In order to control discrimination in a dataset, a first step consists in discovering whether there exists discrimination[2]. If any discrimination is found, the dataset will be modified until Discrimination is brought below a certain threshold or is entirely eliminated[8]. In Economics and Social Sciences, discrimination has been studied for over half a century[1]. There are several decision-making tasks which lend themselves to discrimination, e.g. loan granting insurance premium computing and staff selection[1]. So the decision making utility must be discrimination free. Discrimination is of two types, direct or indirect (systematic). Direct discrimination includes a set of rules (laws) or procedures (events) that explicitly mention minority or disadvantaged groups based on sensitive discriminatory attributes related to group membership[1]. Indirect discrimination includes rules or procedures that are not explicitly mentioning discriminatory attributes, but could generate discriminatory decisions[10]. The literature has given evidence of unfair treatment in racial profiling and redlining, mortgage discrimination, personnel selection discrimination and wages discrimination[2].

In existing passport system, all the processes are time consuming which includes information collection, document submission, document verification, information verification, appointment setup and payment process. All these processes can be done digitally by online passport process. In discrimination process where the attacker can hack user data for bad purpose, can be avoided with the help of anti-discrimination techniques by using online passport process[3].

The human efforts required to issue a passport can be reduced by implementing this online passport system. All the details of user would be transmitted using encryption and decryption techniques so that the privacy of data is maintained[4]. Time can be saved by making the verification process of documentation digital and appointment scheduling easier during passport process. SQL injection attacks allows attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allows the complete disclosure of all data on the

system, destroys the data or makes it otherwise unavailable and become administrators of the database server[5].

III. MATHEMATICAL MODELLING

Let 'S' be the final set of Online passport system

S = {I, O, P, Su, F}

Identify the inputs as 'I' :

I = {A, B, C}

Where

A = {A1, A2, A3, A4 | 'A' is the web application as user's personnel details.}

B = {B1, B2, B3, B4 | 'B' is document uploading.}

C = {C1, C2, C3, C4 | 'C' is payment (Transaction).}

Identify the outputs as 'O' :

O = {X, Y, Z}

Where

X = {X1, X2 …| 'X' is the Response as web application to get data.}

Y = {Y1, Y2 …| 'Y' is the Response as update database}

Z = {Z1, Z2 …| 'Z' is the Response document verified}

Identify the processes as 'P' :

P = { P1(), P2(), P3(), P4(), P5(),P6(),P7()}

Where

P1 : Request on user details.

P2 : Upload required documents.

P3 : Verification of Document.

P4 : Update corrected documents for database.

P5 : Respond for Discrimination taken if any

P6 : Requests for transaction process.

P7 : Set appointment date.

Identify success condition as 'Su' :

Su = {S1, S2, S3, S4}

Where

S1 : Successful registration and login.

S2 : Successful verification of documents.

S3 : Successful transaction.

S4 : Successful booking of appointment.

Identify failure condition as 'F' :

F = {F1, F2, F3, F4, F5}

Where

F1 : Login and registration Failure.

F2 : Document upload and updation failure.

F3 : Transaction Failure.

F4 : Improper knowledge of system.

F5: Unable to access appointment dates.

IV. ALGORITHM

1) Log into the system using two step verification.
2) Data matching by admin to verify the credentials such as UID, DoB, Address entered by the user.
3) This is done by Matching the contents entered with the data base entries dynamically.
4) The user enters the data which is transmitted by encrypting the sensitive credentials such as Adhar UID to preserve privacy of data.
5) The encrypted details are decrypted to verify with the database.
6) Once the documents are verified User proceeds with the further process and transaction.
7) In case of failure to authenticate the documents the user has to reenter the credentials with verified and corrected documents.

V. IMPLEMENTATION DETAILS

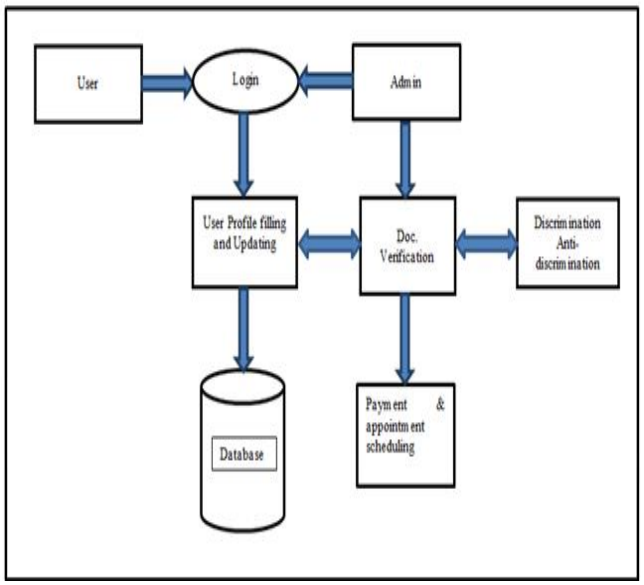

Fig. 1: System Architecture

A. Description:

The System provides an online interface to the user where they can fill in their personal details. The authority concerned with the issue of passport can use this system to reduce their workload and process the application in a speedy manner. The proposed system simplifies this process with online portal where the unique identification number is stored which corresponds to the information of the person. The information includes the name, nationality, address etc. along with attach the copy of the required document required according to the application[6]. The information is transferred to user with the help of online web application.

Modules in the system are as:

1) User module: User login into the system, for authentication user have to save his details and have to upload his document for verification. If user's details and document verification is correct then he will get the appointment for further process.
2) Admin: Admin login into the system, allow user to get access by verifying its data and also keep watch on the user's task of document verification and discrimination.
3) Web application: It helps user by providing the authentication by SQL injection technology. And automatic way to upload, verify and set appointment and payment process for user.
4) Database: Database save the user details for user for authentication purpose so that every time it will check user's saved data for access permission.

This system adopts a comprehensive approach to minimize the manual work and schedule resources, time in a cogent manner. The core of the system is to get the online registration form (with details such as name, address etc.,) filled by the applicant whose testament is verified for its genuineness by the Passport Automation System with respect to the already existing information in the database[4]. This forms the first and foremost step in the processing of passport

application. The application is then processed manually based on the report given by the system, and any forfeiting identified can make the applicant liable to penalty as per the law[7]. After all the necessary criteria have been met, the original information is added to the database and the passport is sent to the applicant.

B. Design:

1) Activity Diagram

- The activities in the passport automation system are login, submit details, get details and verification.
- In the login activity applicant gives username and password and then login into the passport automation system after then fill the required details.
- After the verification procedure is completed successfully the user proceeds with the further process.

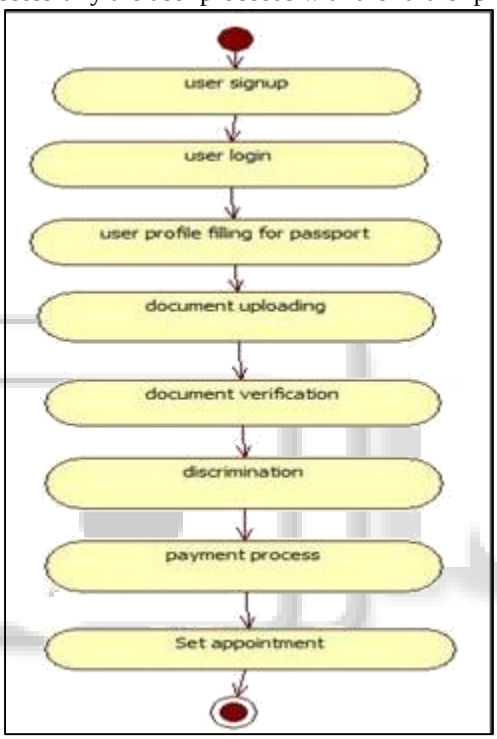

Fig. 2: Activity Diagram

2) Usecase Diagram:

- The actors in use case diagram are user, database, administrator.
- The use cases are signup, Login, update details, verification, payment, set appointment.
- The login use case checks the username and password for user, administrator.
- The verify use case is used for verifying the details by comparing the data in the database.
- The document uploading use case is to update the data in the database.
- And finally the payment gateway use case is used for transaction and set appointment usecase is used for booking an appointment by the user whose application is verifiedsuccessfully by the admin .

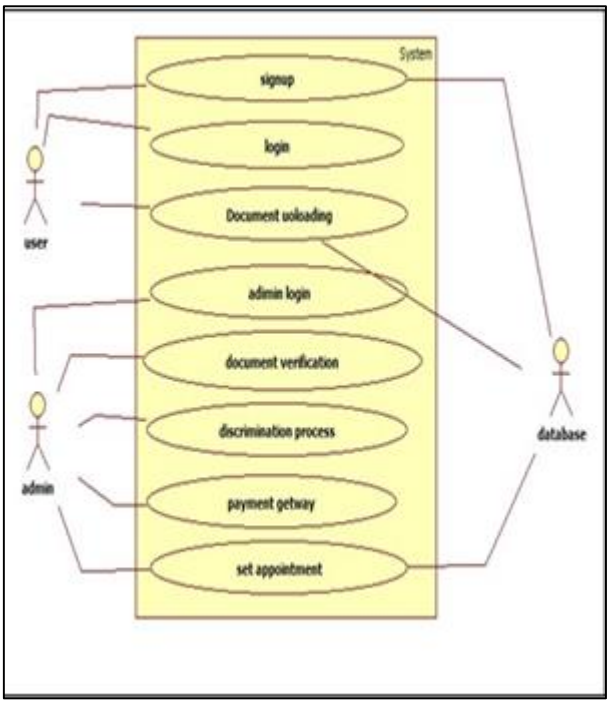

Fig. 3: Use case Diagram

ACKNOWLEDGEMENT

We would like to take this opportunity to thank our guide Prof. Bhagyashree Alhat for the help and guidance. We are really grateful for the support we received. We are also grateful to Prof. Uma Nagraj, Head of Computer Engineering Dept. MIT Academy of Engineering for her indispensable support and suggestions.

VI. CONCLUSION AND FUTURE SCOPE

Thus we have identified and designed a system which is free of discrimination and saves time of user. This system makes the process of issuing passport faster and efficient as well as easier and convenient for the user which will in turn help to reduce human effort.

REFERENCES

[1] S. Hajian, J. Domingo- Ferrer, and A. Martı´nez-Balleste´, "Discrimination Prevention in Data Mining for Intrusion and Crime Detection," Proc. IEEE Symp. Computational Intelligence in CyberSecurity (CICS '11), pp. 47-54, 2011.

[2] D. Pedreschi, S. Ruggieri and F. Turini, "Discrimination-aware data mining". Proc. of the 14th ACM International Conference on Knowledge Discovery and Data Mining (KDD 2008), pp. 560-568.

[3] Dr. Albert B. Jeng, Elizabeth Hsu, And Chia Hung Lin Sponsor: "Should and How CC be used to evaluate RFID based Passports?" ,Telecom Technology Center.

[4] G. Matthew Ezovski, Steve E. Watkins, "The Electronic Passport and the Future of Government-Issued RFID-Based Identification", IEEE, pp. 15-22, 2007

[5] Juels A., Molnar D., Wagner D., "Security and privacy issues in e-passports". IEEE SecureComm, pp.74-88, 2005.

[6] Rima Belguechi, Patrick Lacharme, Christophe Rosenberger, "Enhancing the privacy of electronic

passports".International Journal of Information Technology and Management (IJITM), Vol.11, No.(1/2), pp.122 – 137, 2012.

[7] Marci Meingast, Jennifer King, and Deirdre K. Mulligan, "Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passportand Beyond". Journal of Communications, vol. 2, no. 7, pp. 36-48, 2007.

[8] D. Pedreschi, S. Ruggieri and F. Turini, "Discrimination-aware data mining". Proc. of the 14th ACM International Conference on Knowledge Discovery and Data Mining (KDD 2008), pp. 560-568. ACM, 2008.

[9] S. Hajian, J. Domingo-Ferrer, and A. Martnez Balleste, "Discrimination Prevention in Data Mining for Intrusion and Crime Detection". Proc. IEEE Symp. Computational Intelligence in Cyber Security (CICS '11), pp. 47-54, 2011.

[10] S. Hajian, A. Monreale, D. Pedreschi, J. Domingo Ferrer and F. Giannotti. "Injecting discrimination and privacy awareness into pattern discovery". In 2012 IEEE 12th International Conference on Data Mining Workshops, pp. 360-369, 2012

