International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 7, October 2014, PP 64-70
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Online Crime-Fraud Detection System

Charudatta G. Bangal[1], Mansi R. Mangare[2], Pooja V. Babar[3], Pooja B. Tungar[4]

[1 2 3 4]Department of Compute Engineering, RMD Sinhgad School of Engineering,
Warje, Pune, India

Abstract: *Due to dramatically increased usage of internet we are proposing our system online. Crime identification should be in such a way that the crime measures get reduced in society. Crime identification is the very crucial stage nowadays. Hence we are trying to propose a new web application, to ease of access, by the views of Police and Public. In this paper, not only we are having the crime identification system but also we are going to add some more features like fraud detection system of Government Identity Proof, sim card limit for a single person (9 Sims for each person), Home owner's renter's verification. We are trying to implement this Application in India under consideration of Crime measures and process of crime registration. After successful implementation in India, we will try to make it worldwide.*

Keywords: *Police, Crime Record, Home Owner, Sim Card Company, Renter, Fraud.*

1. INTRODUCTION

Online management of complaint registration and criminal details for fast service. Identity crime is defined as broadly as possible in this paper. At one extreme, synthetic identity fraud refers to the use of plausible but fictitious identities. These are effortless to create but more difficult to apply successfully. At the other extreme, real identity theft refers to illegal use of innocent people's complete identity details. These can be harder to obtain (although large volumes of some identity data are widely available) but easier to successfully apply. In reality, identity crime can be committed with a mix of both synthetic and real identity details.[1] We will discuss some terminology that is used in criminal justice and police departments and compare and contrast them relative to data mining systems.[2]Also we are checking or detecting the frauds of government identity proofs in another domain by storing the original data on the centrally located database of the admin. Now this becomes unsecure to the public to store their personal confidential data online. Hence we are applying a DES algorithm to secure or encrypt such type of confidential data from the admin database. [3] The sim card companies module will consist of options like customer sim card count, customers details those which are required while activating a sim card.[4] The third module is the police department's module, in which the cops are going to update the data in their own database server also and in the admin database also. [5] Next module is house owner's module. In this module we are proposing the advance system for the house owners to register the details of the renter online to the database of the admin. [6]

2. MOTIVATION

As we all know the increasing in the measure in the crime numbers in the India we are trying to do some contribution to help the government authorities and police department by proposing this pepper .A show in the Figure 1 the range of the crime in some cases like murder, kidnap is increasing rapidly from 1983.we are trying to develop a system which will help to the public to register their complaint online within very short time and homeowner can verify their renters document online within short period. In today's police application we can see the details of the register crime but we cannot register the crime compliant [7].so we are trying to develop the application through public can register their

crime complaint online and can see the details of complaints as well as verification of renter's document process can be more easy for the homeowners.

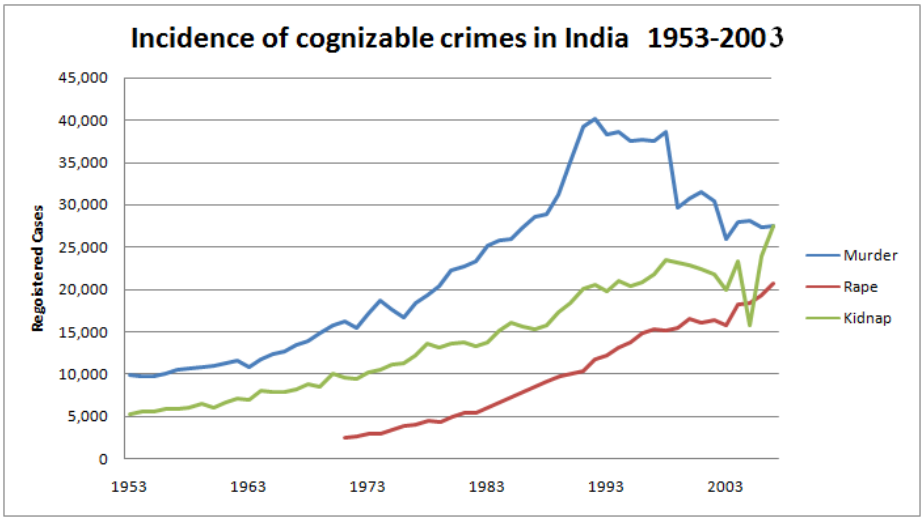

Fig1. *Increasing Criminal Record*

3. AIM

Online management of complaint registration and criminal details for fast service. Identity crime is defined as broadly as possible in this paper. At one extreme, synthetic identity fraud refers to the use of plausible but fictitious identities. These are effortless to create but more difficult to apply successfully. At the other extreme, real identity theft refers to illegal use of innocent people's complete identity details. These can be harder to obtain (although large volumes of some identity data are widely available) but easier to successfully apply. In reality, identity crime can be committed with a mix of both synthetic and real identity details.

4. RELATED WORK

There are no data mining layers of defense to protect against credit application fraud, each with its unique strengths and weaknesses. The first existing defense is made up of business rules and scorecards. In Australia, one business rule is the hundred-point physical identity check test which requires the applicant to provide sufficient point-weighted identity documents face-to-face. They must add up to at least 100 points, where a passport is worth 70 points. Another business rule is to contact (or investigate) the applicant over the telephone or Internet. The above two business rules are highly effective, but human resource intensive. To rely less on human resources, a common business rule is to match an application's identity number, address, or phone number against external databases. This is convenient, but the public telephone and address directories, semipublic voters' register, and credit history data can have data quality issues of accuracy, completeness, and timeliness. In addition, scorecards for credit scoring can catch a small percentage of fraud which does not look creditworthy; but it also removes outlier applications which have a higher probability of being fraudulent.

The second existing defense is known fraud matching. Here, known frauds are complete applications which were confirmed to have the intent to defraud and usually periodically recorded into a blacklist. Subsequently, the current applications are matched against the blacklist. This has the benefit and clarity of hindsight because patterns often repeat themselves. However, there are two main problems in using known frauds. First, they are untimely due to long time delays, in days or months, for fraud to reveal itself, and be reported and recorded. This provides a window of opportunity for fraudsters. Second, recording of frauds is highly manual. This means known frauds can be incorrect [8], expensive, difficult to obtain [9], [10], and have the potential of breaching privacy.

5. EXPLANATION OF IMPLEMENTED METHODS

5.1. Fraud Detection of the Government Identity Proofs

We are checking or detecting the frauds of government identity proofs in another domain by storing the original data on the centrally located database of the admin.

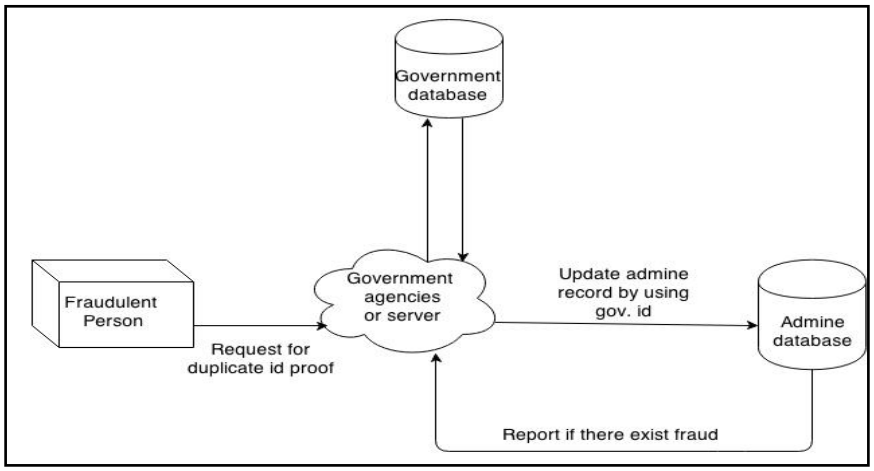

Fig2. *Fraud detection of the government identity proofs.*

5.2. Detection of Total Count of the SIM Cards for Each Customer

Now here in this module, the admin is only going to maintain the total count of the sim cards for a single customer. Whereas the company needs to take permission from the admin for activating a sim card to particular person, after getting the total count of sim card less than 9 from the admin.Then and then only the company will do get activates the sim card for that customer. Also whenever the details of the customers are going to be store in the database the admin will compare it with the criminal's database that either that customer is having any criminal background or not. [4]

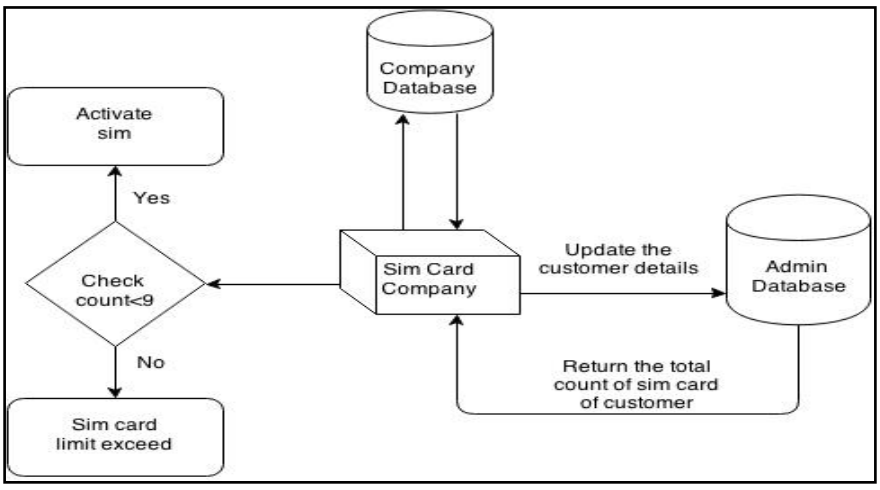

Fig3. *Detection of total count of the sim cards for each customer*

5.3. Police Department

In this module, the cops are going to update the data in their own database server also and in the admin database also. Now what is this data? This type of data which is going to be added by the cops is the criminal record of the police station. This database is managed region vise. The police department's members are going to be have unique user id for login purpose. These registered officers will store the criminal data such as crime, criminal details, etc. on both the database servers. [5]

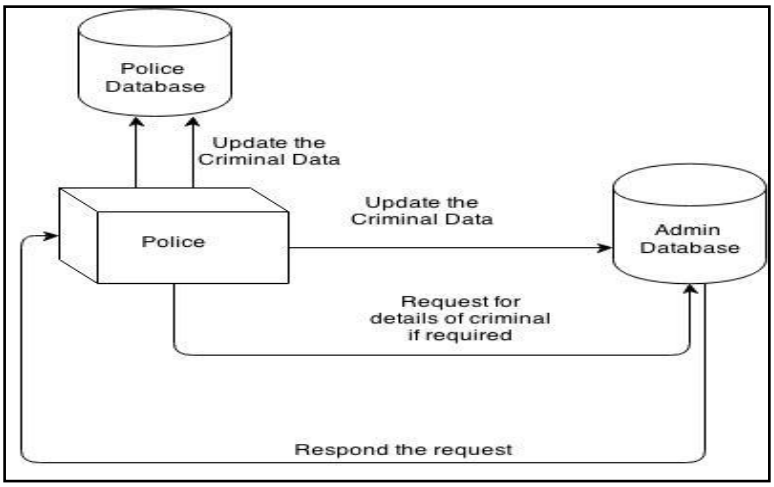

Fig4. *Police Department*

5.4. House Owner

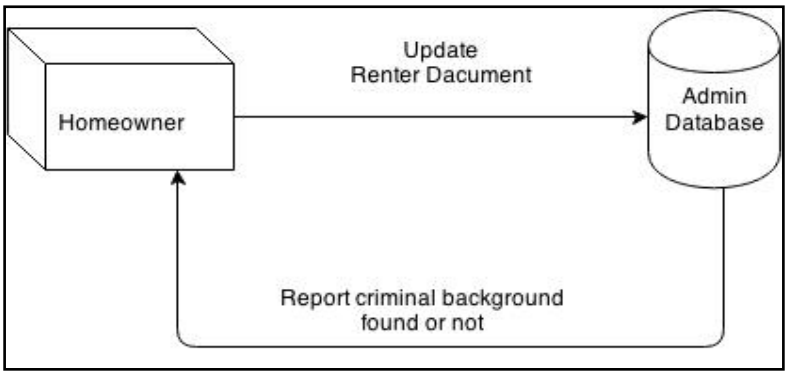

Fig5. *House Owner*

In this module we are proposing the advance system for the house owners to register the details of the renter online to the database of the admin. In real time system, for verification purpose the house owners need to go to the respected police stations. This becomes very tedious job; hence we are implementing it online. The house owner only need to update all the documents of the renter to the admin database, whereas the admin will verify all those documents with the police database and will give review to the house owner.[6]

6. ALGORITHM

6.1. Data Encryption Standard

The **Data Encryption Standard** (**DES**) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. [11]

ALGORITHM

Pseudo Code: Data Encryption Standard

INPUT: plaintext m1 . . . m64; 64-bit key K=k1 . . . k64 (includes 8 parity bits).

OUTPUT: 64-bit ciphertext block C=c1 . . .c64.

1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
2. (L0, R0) IP(m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)

3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:

3.1. Li=Ri-1

3.2. Ri = Li-1 XOR *f* (R i-1, Ki)

where *f*(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:

(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits, T E(Ri-1).

(b) T ' T XOR Ki. Represent T ' as eight 6-bit character strings: T '= (B1 . . . B8)

(c)T " (S1(B1), S2(B2), . . . S8(B8)). Here Si(Bi) maps to the 4-bit entry in row r and column c of Si

(d)T"' P(T"). (Use P per table to permute the 32 bits of T"=t1t2 . . . t32, yielding t16t7 . . . t25.)

4. b1b2 . . . b64 (R16, L16). (Exchange final blocks L16, R16.)

5. C IP-1 (b1b2 . . . b64).

6. End.

7. FLOW OF DATA

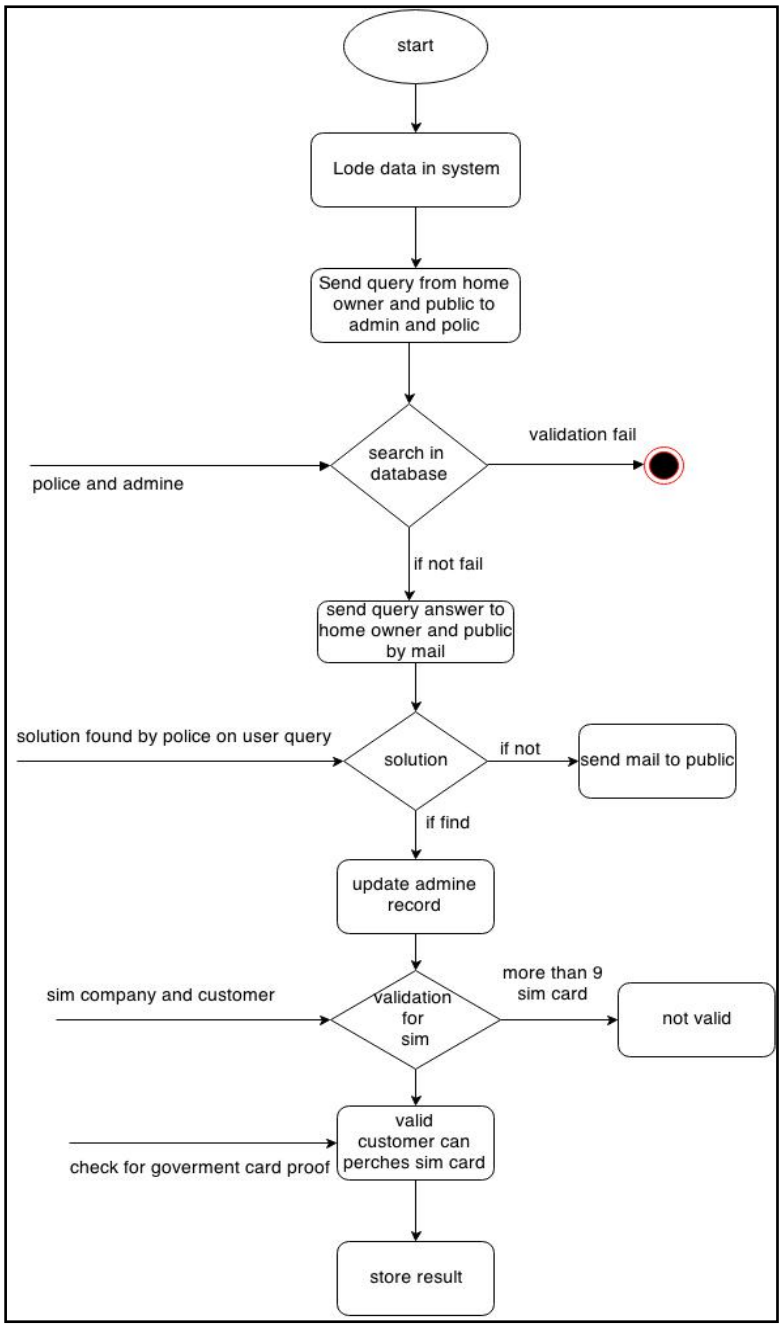

Fig6. *Data Flow Diagram*

8. BLOCK DIAGRAM

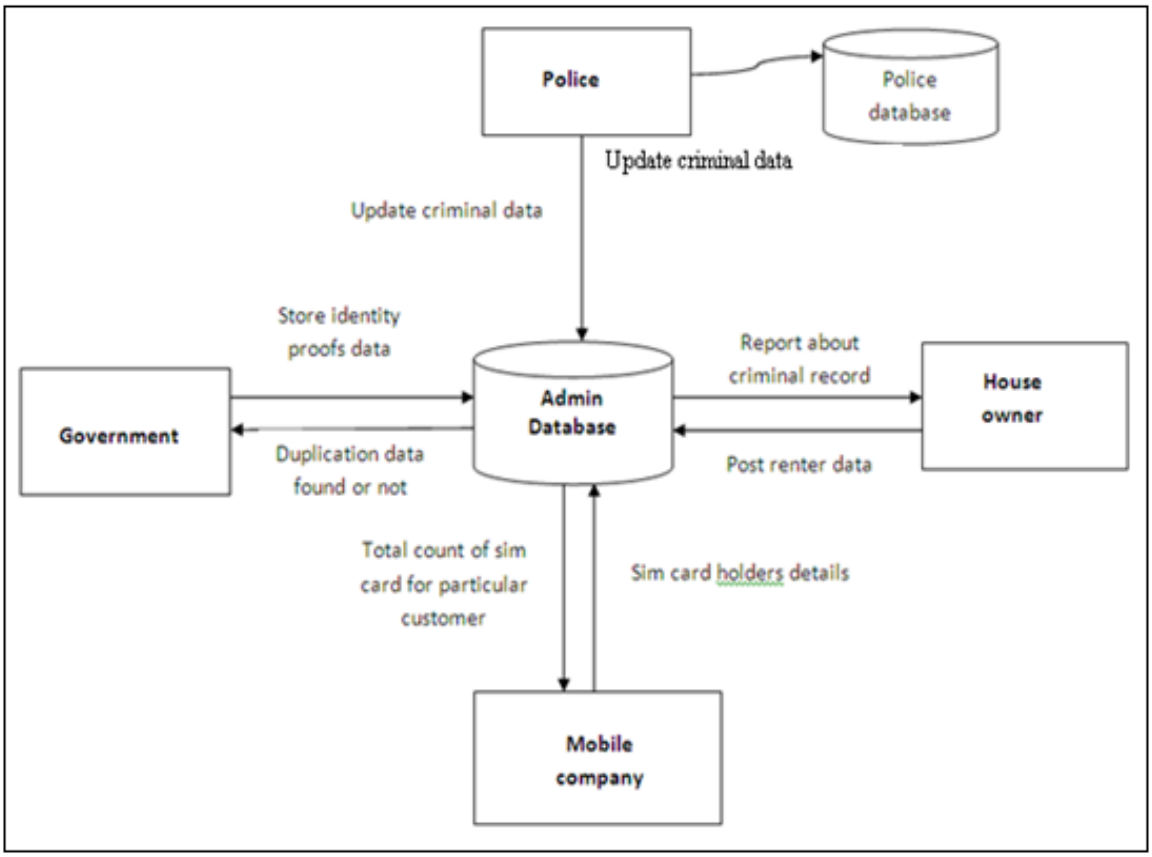

Fig7. *Block diagram*

9. CONCLUSION

In this paper, we have proposed an application of Online Crime-Fraud Detection System (OCFDS). The process of crime registration in India is provided in this application online itself. We have used five different modules as- Police, Public, house owner, sim card company and government agency. We have suggested a method for posting the complaints online, Verifying renters documents online, possibiling to ban more than 9 sim cards for single person, detecting the fraud of duplication of government identity proofs, police can also do store the criminal data onto the database of Police itself and admin which is centrally located. Comparative studies reveal that the Accuracy of the system is close to 75 percent over a wide variation in the input data. The system is scalable for handling large amount of database.

ACKNOWLEDGMENT

The authors would like to thank Department of Computer Engineering, RMD Sinhgad School of Engineering (RMDSSOE).The staff member who have advised us and made their contribution in our project work. The authors would like to express sincere thanks to the editors and reviewers for giving very insightful and encouraging comment

REFERENCES

[1] Clifton Phua, Member, IEEE, Kate Smith-Miles, Senior Member, IEEE, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 24, NO. 3, MARCH 2012

[2] Shyam Varan Nath Oracle Corporation, Crime Pattern Detection Using Data Mining

[3] Data Encryption Standard, From Wikipedia, the free encyclopedia

[4] Subscriber identity module, From Wikipedia, the free encyclopedia

[5] http://india.gov.in/file-complaints-madhya-pradesh-police-online

[6] http://en.wikipedia.org/wiki/Deed

[7] http://www.mahapolice.gov.in/mahapolice/jsp/temp/home.jsp

[8] D. Hand, "Classifier Technology and the Illusion of Progress," Statistical Science, vol. 21, no. 1, pp. 1-15, 2006, doi: 10.1214/ 088342306000000060.

[9] T. Oscherwitz, "Synthetic Identity Fraud: Unseen Identity Challenge," Bank Security News, vol. 3, p. 7, 2005.

[10] P. Brockett, R. Derrig, L. Golden, A. Levine, and M. Alpert, "Fraud Classification Using Principal Component Analysis of RIDITs," The J. Risk and Insurance, vol. 69, no. 3, pp. 341-371, 2002, doi: 10.1111/1539-6975.00027.

[11] https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Data_Encryption_Standard.html

AUTHORS' BIOGRAPHY

Charudatta G. Bangal. Born in Ahamadnagar, Maharashtra, India in 1993. Pursuing Bachelor of Engineering in computer Engineering. His research area of interest is in Computer Networking and Web Designing design and analysis of algorithm.

Mansi R. Mangare Born in Pune, Maharashtra, India in 1993. Pursuing Bachelor of Engineering in computer Engineering. Her research area of interest is in web technology, web developing.

Pooja V. Babar Born in Pune, Maharashtra, India in 1993. Pursuing Bachelor of Engineering in computer Engineering. Her research area of interest is in Web Designing, artificial intelligence.

Pooja B. Tungar Born in Ahamadnagar, Maharashtra, India in 1994. Pursuing Bachelor of Engineering in computer Engineering. Her research area of interest is in Computer Networking, compiler designing and Web Designing.