Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue on Recent Trends in Data Engineering

Volume 4, Special Issue 5, Dec.-2017

Survey Paper on Document Fraud Prevention

Prof. Sarika Zaware[1], Pratik Lodha[2], Parag Sanyashiv[3], Shubham Kadlag[4],Sunil Jagtap[5]

[1]*Head of the Department, Department of Computer Engineering, AISSMS IOIT,Pune*
[2,3,4,5.]*Department of Computer Engineering, AISSMS IOIT,Pune*

Abstract— *Even though world is focusing on being digital still large amount of information or the data is represented by the papers only and that may also contain critical data. Now a days official documents are strongly secured with modern techniques such as artwork or printed pattern, but still paper documents suffer from a lack of security it means that with the high availability of cheap scanning and printing hardware, non-experts also can easily create fake documents. For the many organizations prevention of fraud has become a major concern. The industry understood the problem and is just now starting to act by innovation of new techniques for fraud detection. But as always said prevention is better than cure, we will focus on prevention of frauds, it is the best way to reduce frauds, fraudsters are adaptive and will usually find ways to break the security and circumvent such measures. So, for that purpose we have to make prevention system more and more stronger. In this paper, we present convenient and much more efficient approach for fraud prevention. In our approach, we use the smart card (can be RFID, magnetic tape based etc.). In this smart card, all the educational details can be linked so that the details can be obtained on the go, and hence there is no worries related to carrying your documents all the time with you. Once the organization requires the qualification details we just have to scan the smart card and organization will get all the data. So, the issues related to the forgery or alteration of original documents will be reduced (or you can say fully eliminated!)*

Keywords*-RFID card, UID, Data Encryption-Decryption, AES, Central Database, Embedded*

I.INTRODUCTION

Now a day, paper documents are largely used as it contains the detailed information due to legal reasons. Also verifying educational results has become very important task for recruiters, admission councils, etc. The duplications of leaving certificates allows some to take admission into different degrees from different colleges which is illegal. Rather of all these the paper used for all the procedures are increasing with yearly increasing admissions. At the time of admissions there persist a large number of queue which many times confuses the administrator and can lead to messing of important documents. The document submitted are not every time verified.

So we proposed an experimental smart technology that will help to solve such problems in future. When students fill up forms for board examination and approved, at the time of receiving the hall ticket, a qualification card is provided linking with his respective university. This qualification card will have a unique identification number linked with the PRN or seat number of that particular student. Also, the qualification card information is only readable for that particular student via online login authority. The information like results, government documents (caste certificates, birth certificate, domicile certificates, etc.) will be updated to the profile of that respective card holder at the time of admission by college administrator. The results will be updated to the card holder profile when the results are declared and by the respective board/university. The student can change the respective information if and only if it seems a mistake. The procedure for changing information can be done by requesting an online modification form attached with the scanned copies of documents.

The administrator, at the time of admission will be able to put a status against the leaving certificate block. The leaving certificate block will have N choices which contains engaged, open, etc. at the time of seeking admission at organization/college, they will ask for qualification card and swipes at the POS or keep it with RFID reader, which will retrieve the student information which will reduce the paper use and will not consume excess time required in queue.

The card will be secured with PIN which will reduced the information duplication if lost by an individual. The student has to produce the original documents for cross verification.

Similarly, at the time of recruitment, the job seeker will have produce his qualification card and his respective resume'. The recruiter will read the card with their system and can view the information of qualification updated by university which will reduce the document fraudulent. The recruiter can only view and get the tally of his aggregate required as per company rules.

Every time when card is swiped or contacted with RFID reader will asked for PIN which is to be entered by the respective card holder. Every modification done within the card holder's profile will generate a log file which cannot be deleted unless and until the card authority allows that will indicate if there any duplicate information is updated or not.

Every 10 years, the card will be replaced for maintenance purpose if the card is a magnetic swipe card. For RFID cards will only be replaced if lost, no need to maintain RFID cards unless harsh use of card holders.

Rest of the paper is organized as section II discusses literature survey, section III discusses proposed work, section IV discusses about conclusion followed by references.

II.LITERATURE SURVEY

Multipurpose Smart Card System by Yoso Adi Setyoko and I.G.B. Baskara Nugraha[7]. In this paper, Multipurpose smart card is used to store the identity of user and money/Payment transactions. These transactions are secured with different cryptographic algorithms. This card only contains unique ID. The data associated with that card will be on server for security.

Aditya Bodake, Viraj Baviskar, Ashwini Bodake, Shital Bhoite and Prof. N. J. Kulkarni [11] proposed the concept for various applications can be made together in single smart card with reference to their own paper based on Multipurpose Smartcard System. Since, it not required carry different types of cards everytime. A person has to carry only single card and can use it for different purposes. All the variants like attendance, ticketing and voting can be approached using the smart card which works as a personal Identity.

A Survey on Smart Ration card system using RFID and Biometrics by Smita Khot, Diksha Kamble, Bharti Lokhande, Prachiti Sardar, Tushar Khose. [8] In this paper, the RFID (Radio Frequency Identity) card is used as Smart Ration card. This card will avoid malpractices by consumer and/or shop-keeper. When RFID card is validated by RFID reader, Display device will show the details of consumer with the products to buy and their relative cost.

E-Fraud Prevention based on the Self-Authentication of e-Documents by J. M. Blackledge and E. Coyle.[12] From this paper we have taken the concept of prevention of e-frauds in which using convolution operation, data/document is converted into floating point cipher and then that converted data is embedded behind the host image. Then host image can travel over the internet or network.

K. Eswar Kumar, Ashok Kumar Yadav and Dr. T. Srinivasulu proposed a Smart Card based Robust Security System [10] which specifies that the Smart Cards are secure and as it has small size, it a type of compact space gadget and can be used for various purpose related to security which includes access to database frameworks. Smartcard are “secure” mobile units. Smartcards has a microprocessor chip and memory. This Proposed System stresses on an integrated system for high security areas like nuclear, defense, or any critical entering areas. There are three parameter by which system is secured; they have a rfid or magnetic card on a smartcard, strong password, and particular user identification like facial elements, fingerprint or any biometric entity. This approach can limit the access of the unauthorized person to high secured locations, based on access rights of different persons.

Kamta Nath Mishra proposed a concept which states to merge biometrics into digitalization technology that can improve the credibility of the conventional techniques with reference to Aadhar card based biometric system for security Management. The digital watermarking biometric authentication systems addresses access control and authenticity. We can formulate a reliable and satisfactory individual identification system as the biometrics possesses by embedding biometrics. Since, the conflicts and problems related to intellectual property rights protection can be potentially prevented. Also, the government of United States and Europe decided to include digital biometric data in future ID documents. Aadhar is introduced with the goal of providing a unique identification no. to all the indian citizens with Biometric based UID scheme. For all the money transactions related to all types of purchases, sales, hotel bills, air tickets, money transfer, hospital expenses, etc., can be executed using the Aadhar Number. Hence, these Aadhar System using smartcard will help the South Asian countries in improving their economics and coming out of Corruption.

In the paper on Smart Adhaar Card with RFID, Nawal Kishor, Kalpana Dwivedi, Veer Bhadra Pratap Singh Yadav [1] provides the technology which issued is Radio Frequency Identification technology (RFID) There is an RFID card which is issued to each and every citizen with a unique identification number in it. This card is used as unique identification number in various aspects like epassport, smart parking, hospital details and driving licence which has been explained in this paper.

Performance Analysis of Encryption Algorithms for Security by Madhumita Panda [3]. In this paper the effectiveness and performance of different types of cryptographic algorithms is calculated. This performance analysis can be used to

find better algorithm for future use. In this paper performance is calculated not only for Symmetric (AES, DES, BlowFish) but also Asymmetric (RSA) cryptographic Algorithms.

In the paper on VHDL Based BLOWFISH Implementation for Secured Embedded System Design, Irfan A. Landge and B.K.Mishra proposed a method to protect sensitive data against threat embedded devices are designed with inbuilt security features. The sensitive data is encrypted before transmission so that only authorized user can have access to such information. Hardware implementation of encryption algorithm is helpful in designing secured Embedded System. VHDL based Blowfish algorithm implementation and analysis is discussed in this paper. The algorithm is implemented with different keys and timing required for encryption, decryption are presented.

El-Sayed Abdoul-Moaty, ElBadawy and Waleed A. El-Masry proposed a new chaos of AES algorithm providing in concern of Data Security in the paper on A New Chaos Advanced Encryption Standard (AES) Algorithm of Data Security.[13] The algorithm is based on substituting the Rijndael affine transformation S-box by another one based on chaos theory.[13]The testing of this algorithm is done using the commonly used for determining of whether the binary sequence possesses some specific characteristics that truly random sequence would be likely to exhibit.[13]These are poker tests, runs and frequency, respectively. These statistical tests are performed with the uniform and random distribution plaintext data. The proposed results of chaos AES were compared with normal one and gave a significant improvement for the sequences probability accepted over a wide range of chaos intial conditions. For more security and confidentiality, the sensitivity of initial condition of algorithm gives ability of multiple keys generation.

Suresh Yaram, stated in the paper Machine Learning Algorithms for Document Clustering and Fraud Detection [6] explains the Machine learning plays very important role in processing of large amounts of unstructured and structured data. A set of algorithm is required to get satisfactory and meaningful insights into the data that are helpful in making effective business decisions. The most popular machine learning technique, Document clustering is used to group text documents/unstructured data based on its content and further analyse the data that can be understand the pattern in it. The transformation of unstructured data into structured data can be done in stages by using clustering (k-means) and text mining techniques. Another machine learning technique that can be implemented for use cases is Classification Algorithm. “Fraud detection and cross-sell and up-sell opportunity identification” in financial services, insurance industry and banking. The current paper gives stress on the implementation of both document set of classification algorithm and clustering algorithm(Naïve Bayes, Decision Tree and Random Forest), along with appropriate industry use cases. The performance is also of three classification algorithms will be compared by calculation of “Conclusion Matrix” which actually helps us to calculate the performance measures such as, “recall”, “accuracy” and “precision”.

Apurba Gorai, Rajarshi Pal and Phalguni Gupta, proposed a method on Document fraud detection by ink analysis using texture features and histogram matching [5]. The Gabor filters and Local Binary pattern performs a histogram matching to analyse the document considered by texture features. The extraction of RGB colour information of each word and Texture feature id done from the document. Comparison of normalised histogram is done between two different images of a particular document to generate matching score to take appropriate decision. The method is fully unsupervised since, it doesn’t require any prior knowledge and it consumes less time. As per the advantages of this method, states that it is very efficient.

Summary of Literature survey:
The earlier implemented techniques focused on detection of fraud after it is happened. But we know precaution is always better than cure. So, we have proposed a convenient and efficient technique to prevent the frauds so that the original quality of the file is maintained and so as to make a huge security system to protect the data. We used the concepts of smart RFID card given by above survey for making our system stronger

III. PROPOSED WORK

In this paper, we proposed an experimental smart technology such that data is not directly stored in the smart card but it is stored in the database at the server account based system. This design would use encryption algorithm like AES to encrypt the document during transmission and can be decrypted at end system so provides the better security. When students (user) fill up forms for board examination and approved, at the time of receiving the hall ticket, a qualification card is provided linking with his respective university. This qualification card will have a unique identification number linked with the PRN or seat number of that particular student. Also, the qualification card information is only readable for that particular student via online login authority. The information like results, government documents (caste certificates, birth certificate, domicile certificates, etc.) will be updated to the profile of that respective card holder at the time of admission by college administrator. The results will be updated to the card holder profile when the results are declared and by the respective board/university. The student can change the respective

information if and only if it seems a mistake. The procedure for changing information can be done by requesting an online modification form attached with the scanned copies of documents.

When the RFID card is scanned with RFID reader. The related documents are fetched from the centralized server.

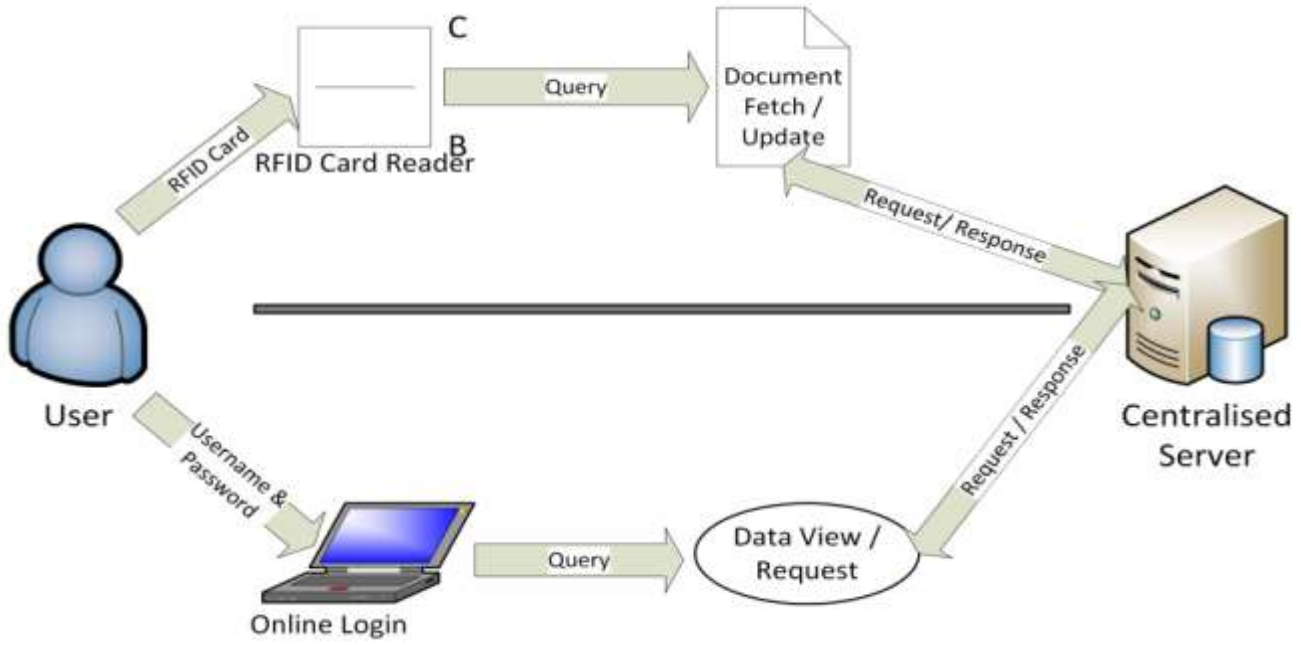

Fig. 1. Data Flow of the proposed method

3.1. The proposed system consists of: User, RFID card, RFID Reader, Centralized server, Security

3.1.1. User:

The user must scan his/her RFID card with reader to fetch the linked documents. If the user wants to see his/her document then user must login to his/her account with the credentials provided throughout the registration method.

3.1.2. RFID card:

RFID stands for **Radio-frequency identification** .It uses electromagnetic fields to identify and track particular objects to which particular tag is attached. This tags has the electronically stored information. There are two types of tags:

1) Active
2) Passive

Passive tags does not have inbuilt energy it gets energy from a nearby RFID reader by interrogating waves (radio). Active tags have a inbuilt power source such as a battery and it can operate from hundreds of meters from the RFID reader

Here we are using passive RFID card that contains only UID (Unique Identifier) which is linked to the centralized server.

3.1.3. RFID Reader:

RFID reader stands for Radio Frequency Identification Reader. It is a device that is used to collect data from an RFID card/tag, which is used to track individual objects. For the transfer of data from the tag to a reader radio waves are used. When the RFID card is scanned with RFID reader, The RFID reader will take associated UID, then with the help of this UID, the related documents from the centralized server can be fetched.

3.1.4. Centralized server:

It is main server meant for saving the information and the documents of user throughout dealings.

3.1.5. To provide security for documents we can use:

3.1.5.1. AES(Advance Encryption Standard):

AES (Advance Encryption Standard) algorithm is 128 bit Symmetric algorithm. The main advantage of AES algorithm is its flexibility. AES supports any combination of data.Key size supported by the AES is 128, 192, 256 bits. The data length allowed by the AES is 128 bit and that data length can be divided into four basic operation blocks. Some transformation Steps are given below

1. Sub byte Transformation
2. Shift rows Transformation
3. Mix columns Transformation
4. Add round key Transformation

Strengths of AES:

1. AES is extremely fast than other block ciphers.
2. Arithmetic operations are not used by cipher.
3. AES allows any sizes of key like 128 bit, 256 bit.

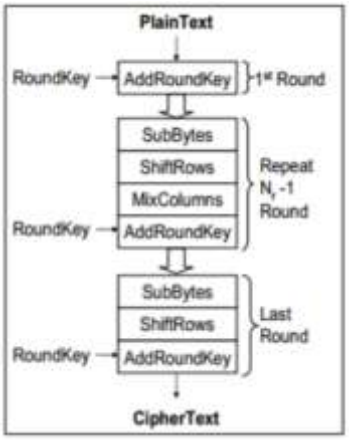

Fig. 2. AES algorithm

IV.CONCLUSION

In this paper, we have proposed Smart Centralized Qualification Card (SCQC) design which will fully eliminate the document frauds as all the original documents are directly linked to the SCQC by the respective university or the board. Implementation of our proposed system takes a step towards the digitalization i.e it makes the work paperless by providing all the original documents without tempering on just one scan of the SCQC.

REFERENCES

[1] Nawal Kishor, Kalpana Dwivedi, Veer Bhadra Pratap Singh Yadav, "Smart Adhaar Card with RFID", ICACTRP 2017.
[2] Kamta Nath Mishra, "Aadhar based smartcard system for security management in South Asia", IEEE 04 May 2017.
[3] Madhumita Pande, "Performance Analysis of Encryption Algorithm for Security", IEEE 26 June 2017.
[4] Irfan A. Landge, B.K.Mishra, "VHDL Based BLOWFISH Implementation for Secured Embedded System Design", IEEE 2017.
[5] Apurba Gorai, Rajarshi Pal, Phalguni Gupta, "Document fraud detection by ink analysis using texture features and histogram matching", 2016 IEEE.
[6] Suresh Yaram, "Machine Learning Algorithms for Document Clustering and Fraud Detection", 2016 IEEE.
[7] Yoso Adi Setyoko, I.G.B. Baskara Nugraha, "Multipurpose Smart Card System", IEEE 19 January 2015.
[8] Smita Khot, Diksha Kamble, Bharti Lokhande, Prachiti Sardar and Tushar Khose, "Online Ration Card System by using RFID and Biometrics ", IJARCCSE 2015.
[9] Pratiksha Divase, Ashwini Thopate, Priyanka Salunkhe, Prof. Jayshree Chaudhari, "Secure Travel System Using Aadhar Card", IJERT 2014.
[10] K. Eswar Kumar, Ashok Kumar Yadav, Dr. T. Srinivasulu, "Smart Card based Robust Security System", IJEI 2013.

[11] Aditya Bodake, Viraj Baviskar, Ashwini Bodake, Shital Bhoite, Prof. N. J. Kulkarni, "Multipurpose Smartcard System", 2012 IJARCET.
[12] "J. M. Blackledge, E. coyle, "e-Fraud Prevention based on the Self Authentication of e-Documents", IEEE 08 March 2010.
[13] El-Sayed Abdoul-Moaty ElBadawy, Waleed A, El-Masry, "A New Chaos Advanced Encryption Standard (AES) Algorithm for Data Security", IEEE.
[14] Gaurav Gupta, Sanjoy Kumar Saha, Shayok Chakraborty and Chandan Mazumdar , "Document Frauds: Identification and Linking Fake Document to Scanners and Printers" ,IEEE 2007.
[15] Deep Vardhan Bhatt, Member, IEEE, Stefan Schulze, and Gerhard P. Hancke, Senior Member, IEEE, "Secure Internet Access to Gateway Using Secure Socket Layer", 2006 IEEE.

