A Noval Approach For Passport Digitization Using 256-Bits Encryption Technique

Vivek N. Waghmare[1], Ranjit A. Pandit[2], Savita S. Khandbahale[3], Sunanda S. Gaikwad [4]
[1, 2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] Sandip Institute of Technology and Research Centre, Nashik,India

Abstract- *Digitization of Passport (D-Passports) is widely deployed in most of the developed countries. It stores the individual information on a tiny Radio Frequency Identification (RFID) chip. The stored information is used to authenticate the identity of individual via wireless interface to reader. In recent scenario, various countries of government have identified the multiple fake passports. Usually, these fake passports are used for performing illegal activities across the country boundary. Consequently, this issue becomes threats for the nation. Based on this issue, we propose a solution known as D-passport. D- passport uses two technologies viz. RFID and Smart Integrated Circuit (IC) memory. The passport card generate encrypted key using a combination of RFID, passport number, passport card number and IC ID. Further, this encrypted data is send to the server and the server decrypts the data. The individual user verifies his/her data with the server data and then sends it backto the client machine. The theoretical analysis shows that our propose approach enhances the security measure, and countermeasure threat andattacks.*

Keywords- Cryptography, D-Passport, Integrated Circuit (IC), Radio Frequency Identification(RFID).

I. INTRODUCTION

A passport is a travel document, usually issued by a country's government that certifies the identity and nationality of its holder primarily for the purpose of international travel [1]. A passport is merely an identity document that is widely recognized for international travel purposes, and the possession of a passport does not in itself entitle a traveller to enter any country other than the country that issued it, and sometimes not even then. Many countries normally require visitors to obtain a visa. Each country has different requirements or conditions for the grant of visas, such as for the visitor not being likely to become a public charge for financial, health, family, or other reasons, and the holder not having been convicted of a crime or considered likely to commitone[2][3].

The main functionality of this approach is to access the passport details of a passport holder through RFID technology. For this purpose the authorized person is given an RFID card. This card contains an integrated circuit that is used for storing, processing information through modulating and demodulating of the radio frequency signal that is being transmitted. Thus, the data stored in this card is referred as the passport details of the person. Proposed approach uses smart card which consists of Integrated Circuit (IC) memory chip and RFID tag. This memory chip contains combination key (ComboKey) which will form by combining three keys i.e chip number, passport number and passport card number. This combination key is in encrypted form which will be used on the network. At the immigration check smart card is scanned by the RFID receiver and the user verification process will be done. The ComboKey will get verified with the passport server. The Combokey will be get decrypted and the following data will be get verify with the passport database.

The system will send back the passport holder's details if he is authorized, else the negative acknowledge will be sent. This system will deploy widely all over the globe. The countries which are associating with International Civil Aviation Organization (ICAO) they have set predefined set of protocols, and the associating countries will follow that method. Every passport user has to upgrade his passport into passport card. Though it will be little time consuming, but the result of this practice will enhance thesecurity.

II. RELATEDWORK

In last few years, we have observed many cases regarding duplicity of passport. General Directorate of Residency and Foreigners Affairs Dubai (GDRFA) has detected 718 fake passports, 23 altered passports and 417 impersonation cases from January 2016 to 2017 [4]. In year 2016, 48 fake passports were identified by Kerala police and many more cases all over the world [5]. These reports are only which were found during raid and many of them still are unidentified. To overcome the problem, we came up the solution in which the existing passport will be verified by the passport card and the authentication will be done by server. Though every passport number will be unique and it will verify every time with server.

FadiHamad, Jamal Zraqou, AdiMaiita&AnasAbu Taleb,[6] they have mentioned that, Since 2004, two main ePassports standards dominated the international landscape, the International Civil Aviation Organization Public Key Directory (ICAO PKD) E-passports and Extended Access Control (EAC) E-passports. These two standards provide sets of guidelines and protocols specifications to standardize and secure ePassports. The ICAO PKD protocol acts as a central broker, where certificates and provocation list are exchanged to ensure that technical standards set by ICAO are adhere; thus, interoperability is achieved and maintained [7]. The EAC Terminal Authentication (TA) protocol enables the RFID chip to verify whether a terminal is entitled to access the sensitive biometric data [8]. To protect travelers privacy, terminals has to show a valid certificate for the access of the chipdata protected by EAC. In integrated terminals, the Hardware Security Module (HSM), which contains the private key of the terminal, is physically part of the reader [9]. As a result, the use of compromised EAC terminal is even more challenging. Before engaging the TA protocol, ePassport tag must be detected through valid reader, otherwise engaging the TA protocol becomes a serious threat to passengers privacy. For this reason, a procedural and technical security mechanism, which it is the scope of this study, must be implemented to provide a secured and efficient reader authentication that protects the E-passport tag from releasing its data to an invalid reader.

V.K. Narendrakumar&B. Srinivasan [10] they have proposed a biometric passport which contains biometric information which validates the authorized user. This system uses contactless smart card technology, containing a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport. Electronic passports include contactless chip which stores personal data of the passport holder, information about the passport. It contains cryptographic mechanisms which protects security of the document and privacy of the passport holder. In that, the passport's information is printed on the data page of the passport and also stored in the chip. To authenticate the data they have used Public Key Infrastructure (PKI) in the passport chip. They used Basic Access Control (BAC) which protects the communication channel between the chip and the reader by encrypting transmitted information. If BAC is used, an attacker cannot easily access transferred information without knowing the correct key. It also uses Active Authentication and Passive Authentication. Passive Authentication (PA) which prevents modification of passport chip data. The chip contains a file (SOD) that stores hash values of all files stored in the chip (picture, finger print, etc.) and a digital signature of these hashes. The digital signature is made using a document signing key which itself is signed by a country signing key. If a file in the chip e.g. the picture is changed, this can be detected since the hash value isincorrect.

Rima Belguechi, Patrick Lacharme, Christophe Rosenberger [11] have addressed the problem of privacy in the current architecture in electronic passports for the storage and transmission of bio-metric data such as fingerprints. They have proposed a new solution combining cryptographic protocols and cancelable biometrics. The individuals biocode in protected by cryptographic keys exchanged by the PACE protocol. They put into obviousness the benefit of the proposed solution in terms of security and privacy. In this electronic passport system biometric technologies are used to verify the identity of an individual (i.e. to perform an authentication) or to determine his identity. The major reason for this widespread usage of biometrics is that this technology provides the strongest proof of the physical identity of a person.

T. S. Muthu Kumaran, M. Suriya, S. Karthik [12], they tried to replace the travel document (passport) using bio-chip which is provided with unique id. To combat international crimeand protect against forgery, countries around the world need to use biochip which consists of complete information of a person. The biochip implant system is actually a fairly simple device. Todays, biochip implant is basically a small (micro) computer chip, inserted under the skin, for identification purposes. The biochip system is radio frequency identification (RFID) system, using low-frequency radio signals to communicate between the biochip and reader. Visual Studio includes a code editor supporting IntelliSense as well as code refactoring. The integrated debugger works both as a source-level debugger and a machine-level debugger.

PrashantShende, Pranotimude, SanketLichade[13], the e- Passport contains an RF transponder, implemented as a contactless smart card, embedded in the cover of each passport. This transponder contains the information currently on the data page of the passportname, birth date, country of citizenship, passport number, etc.with the image of the passport holder stored as a JPEG file. The selected technology is a passive International Organization for Standardization (ISO) and RF transponder with 64kB of on-board memory. Using an embedded electronic chip in the passport to store the information from the passport data page will enhance the security of the document and is expected to benefit travellers by improving the ability of border officials to verify personal identities. The department plans to use this format because of the enhanced security features. The chip is passive and contains no power source, as it receives power from the RF fields produced by the reader. The standard does not explicitly

address the read range of the chip, but it is generally accepted that the read range will be a maximum of 4 inches (10cm) from reader to chip. Radio Frequency Identification (RFID) technology has existed fordecades.

Shruti Sharma, HarshaliZodpe [14] E-passports are a more secured and are denoted by a symbol. E-passports contain a small chip which stores the data of passport holder. To protect this data cryptography is widely used.

This paper shows the comparison of modular multiplication methods used for RSA algorithm for 1024 bit key length. Xilinx ISE 14.3 platform is used to execute this encryption and decryption process. E-passport is majorly used in various countries; some countries are at the verge of changing their traditional passports to e-passports due to upgraded security in them. In this approach, an asymmetric cryptography, RSA algorithm invented in 1977 by Rivest, Shamir and Adleman is used. AdethyaSudarsanan [15], this cloud computing based approach involves standards and technologies like NFC, QR Codes and Cloud Infrastructure to design a mobile application which will perform desired functionalities. Cloud Storage is used as a reservoir to store the artifacts used by the application. Development and testing of the application is initially carried out on emulators or simulators followed by testing on real handsets / devices. The proposed system suggests that traditional passport is replaced by an application that will act as passport. This application is designed to work on all devices and allplatforms.

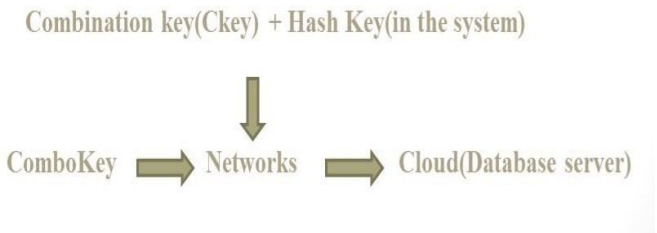
Ajit Singh and Prof. Rahul Rishi [16] they mentioned more robustic mutual authentication and key exchange protocol based on Elliptic curve discrete logarithm problem is described. In this protocol is a two party protocol in which first server authenticates itself to the client and after that client authenticate itself to the server over an untrusted and unsecured network before the session key generation. no one has been proposed which provides forward secrecy and resistant to dictionary attack in an efficient manner. This paper provides a new efficient and robustic mutual authentication and session key exchange protocol for high security web applications. They propose a new elliptic curve based mutual authentication and session key establishment protocol with the features of full forward secrecy and ability to ensure strong identity privacy. The proposed protocol is based on Elliptic curve digital signature algorithm that is applied to prime order elliptic curve having large embedding degree. As we use elliptic curve cryptographic system with higher strength per key bit, the protocol has the benefit of higher computational speed, lower power consumption, smaller bandwidth requirement and a smaller size message exchange between the communicatingparties.

III. IMPLEMATIONDETAILS

Passport is an official travel document issued by a country's government to its citizens. Along with a valid passport, the user should also possess a document to enter the destination country. This document is called Visa. Visas are usually issued as stickers which are affixed to the passport. These essential travel documents need to be carried every time one travels to another country. The existing system is time consuming and it is not reliable. Even in some cases fake passport are identified and some may success to eliminate from the verification. for this problem we have done brain storming and we got a solution by using smart card. This will enhance the security of passport system while having communication between the database and end node.

Instead of using booklet the proposed system will be using smart card with a memory chip which will store following data: Chip number (chip no.) is given by the company at the time of manufacturing and it is not repeated. Passport number (Passport no.) is assigned by the Passport SevaKendra. Every smart card has unique number (Passport card no.) and that unique number will act as passport card no. which will be visible on the card with users name. With the help of this three numbers we will make a combination key(CKey).

This Combination Key (CKey) will get generated at the time of scanning the card with help of intermediate machine. With the help of Hash key the Combination key will converted into theComboKey.



This Combokey will be passed through over the network for the verification of passport. The passport number will be stored in Pending Passport No Queue class which digitize passport is not created yet. The passport card generator will fetch the upcoming passport number from the queue. Later the card will be scanned by the system. The system will retrieve the passport card number and the IC memory Chip number after the scanning. Then the all these three entities (Passport No., Passport Card No., IC memory chip number) will be encrypted by the DES 64- bits encryption algorithm. The three ciphers key (PreCombokey)

will be combined into one single block. Then the AES 256-bits encryption algorithm will be performed [17]. The Figure 1 shows the architecture of D- Passport system.

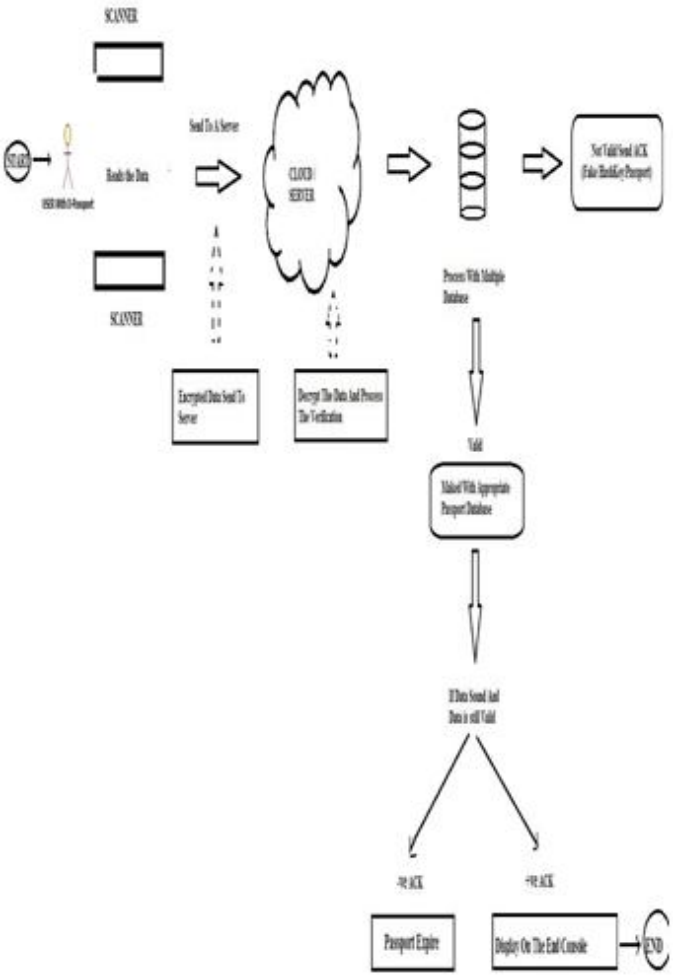


Fig. 1. Proposed Architecture of D-Passport System

The passport holder (owning digitize passport) will pass through the RFID scanner. The RFID number will be scanned and authenticate it from the Server. Later, if the RFID is valid then it will check for the ComboKey which is stored in the IC Memory chip of the passport card. The ComboKey will be forwarded to the server. It will decrypt the ComboKey into Three entities which are Passport Number, passport Card Number and the IC Chip Number by using AES 256-bits decryption algorithm. This all three entities are in encrypted form. The whole ComboKey block will be divided into the 3 block at the 64-bits of interval each. These are the Cipher text of three entities. These three entities will be decrypted individually by DES 64-bits decryption algorithm. After decrypting all these keys, they will be verify with the organization database. If the all term matches successfully then the user details will forward at the verification center and display it at themonitors.

Proposed Algorithm for Encryption

Input: Character>>PassportNo;12digit>>PassportCardNo;20character>>ChipNo.

Output: Ciphertext (ComboKey)

1. Start.
2. Get the Passport Number from thelist.
3. Scan the Passport card and get its Passport card Number and IC memory chipNumber.
4. Apply 56-bits key DES encryption algorithm on all these three entitiesindividually.
5. Now combine all this three entities and encrypt it by AES encryption
6. Algorithm using 256-bits key.
7. Burn/Write this cipher key (ComboKey) on the IC memorychip.
8. Assign RFID card number with the key insystem.
9. End.

Proposed Algorithm for Decryption

Input: Cipher text (ComboKey)

Output: Character>>PassportNo;12 digit>>PassportCardNo;20character>>ChipNo.

1. Start.
2. Scan the card.
3. Verify the RFID card number associate card in the system.
4. Scan the ComboKey.
5. Decrypt it using 256-bits AES decryptionalgorithm.
6. Divide the decrypted text in 64-bitsblocks.
7. Three entities will be derived after diving theblocks.

V. CONCLUSION

The proposed system focuses on all technical aspects of digitization of passport. The Cryptography method used for encryption will enhance the security of data. The proposed system will be not easy to temper. The proposed passport card if get copied, it is easy detect the fake one. The existing fake passport holder will be getting identified, after updating of the system. The international crime operating with fake passport will be getting in limited.

REFERENCES

[1] FadiHamad,JamalZraqou,AdiMaiita,AnasAbuTaleb,"ASc ure Authentication System for ePassport Detection and

Verification", 2015 European Intelligence and Security InformaticsConference.

[2] Kenk, V.S., Kriaj., J., truc, J. and Dobriek S., Smart Surveillance Technologies in Border Control, in European Journal of Lawand Technology, Vol 4., No. 2.,2013.

[3] Bundesamt fur Sicherheit in der Information Stechink(2010), "Advanced Security Mechanisms for Machine Readable Travel Documents- Extended Acces.

[4] Department of Homeland Security US-VISIT Program. URL:(http://www.dhs.gov/files/programs/USU.shtm),2010.

[5] V.K. Narendira Kumar and B. Srinivasan, "Design and Development of E-Passports using Biometric Access Control System, International Journal Of Advanced Smart Sensor Network Systems(IJASSN),Vol 2, No.3, July2012.

[6] Rima Belguechi, Patrick Lacharme, Christophe Rosenberger, "Enhancing the privacy of electronic passports", hal-00984023, 26 Apr 2014.https://hal.archives-ouvertes.fr/hal-00984023.

[7] T. S. MuthuKumaran, M.Suriya, S. Karthik, " Replacing E-Passport Using Bio-Chip ",International Journal Of Scientific Research, ISSN No 22778179..

[8] PrashantShende, Pranotimude, SanketLichade, "Design and Implementation of Secure Electronic Passport system, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print):2320-9798.

[9] Shruti Sharma, HarshaliZodpe, "Implementation of Cryptography Algorithm for E-Passport Security", Department of Electronics and Communication, Maharashtra Institute ofTechnology.

[10] Adethya Sudarsanan, "CloudPass a passport system based on Cloud Computing and NearField Communication", CognizantTechnology Solutions India Pvt.Ltd.

[11] Ajit Singh and Prof. Rahul Rishi, " A Novel Approach towards Mutual Authentication and Key Exchange Protocol based on Elliptic Curve", Second International Conference on Advanced Computing and Communication Technologies, IEEE,2012.

[12] V.K. Narendira Kumar, B. Srinivasan, P.Narendran, "Efficient Implementation of Electronic Passport Scheme Using Cryptographic Security Along With Multiple Biometrics", I.J. Information Engineering and Electronic Business, 2012, 1,18-24.

[13] ICAO Technical report," biometric passport machine readable travel documents, Seventh Edition, ICAO2015.