International Journal of Pure and Applied Mathematics
Volume 118 No. 7 2018, 447-454
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

NFC based Anti-Counterfeiting Scheme for Certificates Identification and Verification using a Smartphone

Yeshiwas Hunegnaw
Computer Science and Engineering
Symbiosis International University
Pune,India
yeshiwas2014@gmail.com

Pooja Bagane,Advisor
Computer Science and Engineering
Symbiosis International University
Pune, India
pooja.bagane@sitpune.edu.in

ABSTRACT: **- Now a day, counterfeiters are widespread over the world, almost all states have been lost a huge amount of revenues per year. To overcoming this problem the researchers were designed solutions according to Internet of Things (IoT) technology, especially barcode, Radiofrequency Identification (RFID), and Quick Response (QR) codes for transfer secret information from manufacturer to customers. however, some of these technologies are unable to support security algorithm rather the RFID, but it needs unaffordable physical RFID reader device so, not yet sufficiently designed an easily accessible well-secured systems, for keeping originality of documents such as educational certificate, driver licenses , investment agreement documents, marriage certificate, passport and such like valuable documents. Hence, we proposed to design this security scheme protocol through Near Field Communication (NFC) tag, the tag being able to store secret information and the user to be read that secret information through their NFC enabled smartphone for checking the corresponding document is counterfeited or not in offline environment. It will use the lightweight cryptographic algorithm and random number generating by the reader and send it to tag for mutual authentication between the tag and NFC reader which is a user smartphone. In addition to that, it will use the third trusted governmental party for trustfulness. This system isrelatively efficient with respect to computation and communication costs. Finally, for the demonstration of practicality of the scheme, we evaluate it using simulation.**

Keywords:-Authentication, Anti-counterfeiting, Documents or certificates anti-counterfeiting, Security with Internet of Things, Near Field Communication.

I. INTRODUCTION

NFC based marketing size of payment services is expected to be increased to $180 Billion in the year 2017 [1], whereas, the ICC (International Chamber of Commerce), OECD (Organization for Economic Cooperation and Development), Vandagraf predict the counterfeiting and piracy a $ 1.3 trillion global financial loss, projected to reach $ 2.8 trillion by 2020. While the wireless technology is rapidly growing to develop in this era, therefore the security should be unquestionable and hot necessary issues to make efficient and threat free a comfortable communication environment. In the NFC based communication environment, the Trusted Service Manager (TSM) is responsible to manage the authentication process.

NFC Jointly developed by Philips and Sony, based on RFID technology at 13.56 MHz of the standard ISO 18092 and backward compatible with IS0 14443. It refers to contactless technologies that identify items over a range of distances, in most cases without the need for a battery. NFC tags combine a tiny microchip with an antenna that picks up electromagnetic energy beamed at it from a reader. When a tag senses the beamed energy, the tag sends its unique identifier to the reader. The unique identifier can be tied to other types of information, stored in the tag's memory, or can be connected to the cloud, so it's possible to identify, authenticate, track, trace, and interact with individual The transmission capacity of NFC technology is limited as its operating frequency is 13.56 MHz with transmission speed ranging from 106 Kbps to 424 Kbps up to 10cm or 4 inch [2].

Highly valuable documents should require a quit keeping from counterfeiting publication. Those documents such as educational degree certificate, birth certificates, passports, marriage certificates and driving licenses should be improved and secure their originality**.** The existing RFID based systems have been required the 3rd independent physical component which is RFID reader. RFID tag reader is not available on the smartphone [3], because of this reason RFID based authentication systems are not accessible for everywhere. Aparna.R and Ravi.V[8], the proposed scheme used less capacity of Random Number generator(RNG) security bits which is 16, therefore this is vulnerable to counterfeiters or attackers easily to break the communication. NFC enabled tags; a simple tap of with an NFC smartphone is all it takes to verify authenticity, so everyone – even consumers – can join the fight against fakeness.

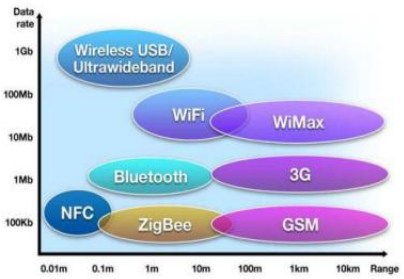

Figure 1. Distance and data rate difference of NFC with other existing wireless technologies (NFC Forum)

PAPER STRUCTURE

In Section II, discuss for motivational idea of this research paper. Next, on section III, review of an existing related anti-counterfeiting techniques. Section IV discusses about the new proposed scheme with our intended contribution. Section V gives the description of the methodology and techniques of various phases related to the proposed scheme. The acknowledgment is given in Section VI. Conclude discussion of the paper at Section VII. Finally, references of the reviewed papers have been included.

II. MOTIVATIONAL IDEA

Now a day, numbers of counterfeiters are dramatically increased throughout the world. Hence, this situation has a negative impact on country's growth economy. Especially, in developing countries such like African; it is a great challenge for their economic, social and political developments because of lacking qualities. Additionally, it is also a new and hot issue of future research area.Therefore, we are selected this topic based on the above mentioned reasons.

III. RELATED WORKS

The NFC topic is still relatively new in the literature sense, and the idea in its basic form developed from the older RFID communication systems. The advancement in mobile computational power has facilitated the emergence of new application. Due to this reason, most of literatures deal with application development and how it utilizes NFC systems in different areas. due to the nature of NFC systems, the close proximity provides a natural immunity against several attacks, and partially due to the fact that NFC systems are still new and not widely used in different areas of communication and commerce.

A.Al-Ghaihebet al. [10] proposed the NFC technology utilization with security analysis using the widely accepted Real-Or-Random (ROR) model proves that the proposed scheme provide session key(SK) security, in addition to that they have used a one-way hashing function. However, their scheme has trustless, because of replying notification of medicine geniuses might be delivered by counterfeiters since their system deployment couldn't allocate a third trustful authorized key management.

C.Wenxue et.al. [1] Reviewed a design traceability system using the combination of RFID and barcode for traceability of vegetable products from planting to distribution and delivery. They proposed to use RFID for the entire enterprises while the barcode to be applicable for outside of the enterprise.Using traceability code accordance with EAN/Ucc-128 code format and printed on traceability tags to be attached to product packaging, however,Barcode is a traditional track and trace techniques and it holds data statically and also it does not provide a security mechanism therefore, this has a wide vulnerability problem to counterfeiters.

S.M.Qasim et al. [4] designed the scheme working at offline in consumer level for detecting counterfeit products through the integration of NFC tag with EPC tag. The embedded tag will be read at anywhere using consumers' NFC enabled mobile without online server connection. They had to provide a dual layer verification mechanism to a consumer, first display product verification on customer's cell phone for visual verification against the actual product. After successful verification a Cryptographic challenge-response protocol is executed to authenticate the product based on Public key Infrastructure (PKI) and Public key cryptosystem (PKC). Since the scheme works on offline the customer might not trust the scheme because the product may be produced by counterfeiters, therefore in this scheme, there is not an evidence to ensure the product is genuine or not? Counterfeiters may have this kind of authentication system for their fake products that work as legal.

Therefore, to overcome this kind of weakness the third authorized governmental risk taker organization is required and the scheme should provide online service connected to the authorized organization's server to improve consumers' belief.

W.H.Leeet al. [7] the aim of this designed framework is to provide a secure smart card and utilize discrete cosine transform techniques to embed an invisible watermark into a digital photo to achieve data protection and verification.They have used two layered image protection mechanisms, those are embedding watermark process and extracting watermark data from digital images using discrete cosine transform techniques for embed a protected anti-counterfeiting metadata into digital image by invisible watermark technique. This technique includes forward and reverse discrete cosine transform techniques.

A.Goswamiet al. [9] Viewed the recently, a pseudonym-based NFC protocol (PBNFCP) has been proposed to withstand the security pitfalls found in the existing conditional privacy preserving security protocol (CPPNFC).because of this the researchers aimed to propose a new secure and efficient authentication protocol (SEAP) for NFC applications using the new defined lifetime based pseudonyms to withstand the security drawbacks found In PBNFCP. They have used Security protocol based on asymmetric cryptography using elliptic curve cryptography (ECC) mechanism and a life time-based pair of pseudonyms with private key for mutual authentication between two users through secure communication with in specified life time in order to minimize impersonation attacks. This has also a similar weakness as [10] which is un trustful becausethe counterfeiters unknowingly design a hidden system which is doing the same task as the legitimate system so, in this situation the user get confused.

IV. THE NEW PROPOSED SYSTEM

An International Anti-Counterfeiting Coalition Estimates those sales of counterfeits are a $600 billion a year problem that causes losses in revenues, brand damages, and that can even be hazardous to health and well-being in the case of faked drugs or faked parts in the airline or car industries [14]. Now a day, many countries have faced forged documents fabrication challenges too. Such as passport, educational certificate, driving licenses, Identification cards, marriage certificate, birth certificate as well as financial related documents have a threat of counterfeiting risk. In general, counterfeiting documents are causes for a serious threat to the government on country's development.

There are four useful technologies to trace and track items' current location and status, those are Barcode, QR, RFID and NFC, however, the first two technologies are working statically with holding limited data whereas the remaining are working dynamically. However, most of RFID based tracking systems are required unaffordable extra RFID reader device. Since, now a day NFC enabled smartphones are widely producing by manufactures therefore, this is the best choice of preventing counterfeiting problems at every time in everywhere by everyone with minimum cost requirement.

Attributes	**Technologies**			
	Barcode	***RFID***	***QR code***	***NFC Tags***
Data capacity	>20 characters	Maximum 8000 bytes	Maximum 2953	Maximum 1.6 MB
Direct line of sight	Requires line of sight	Does not direct require line of sight	Requires direct line of sight	Does not direct require line of sight
Reusability	Has to be reprinted each time	Rewritable/reusability	Has to be reprinted each time	Rewritable/reusability
Durability	Can't be used when scratched/stained	Can be used even when scratched/stained	Wrinkled tags can't be used	Can be used even when scratched/stained

Table.1 different technologies capacity comparison

In the existing traditional RFID or Barcode based systems are being required three independent physical components, such as RFID interrogator, RFID Transponder, and Controller. The RFID tag interrogator /reader is not affordable and unavailable on smartphones [6], because of this reason RFID based authentication systems are not accessible for everywhere. Even the new NFC based researches for prevention of counterfeiting problems have some pitfalls. Now, this proposed security scheme protocol has worked on NFC enabled mobile the semi-offline environment which is accessible to everywhere then users can easily identify their own or others certificate's genuineness through stored secret data from tag's memory which is embedded with the published certificates that helps to prevent or mitigate the counterfeiting threats. It will use the low communication as well as computation costs algorithm based on compatible of tag's capacity.

Symbol	**Description**
SK	Trusted organization's secret key
RK	Randomly generated key
E_{SK}	Encryption by trusted organization's secret key
NFC	Near field communication

M1	First encrypted message
M2	Second encrypted message
M3	Third message
E_{RK}	Encryption by random generated key
IDKj	Tag Identification number
Rr	temporary random numbers

Table 2:- *Notations used in our scheme*

V. METHODOLOGIES

a. Techniques

The new proposed scheme to be used a short and quite useful algorithm or techniques to achieve proposed goal within less time of computation, as well as communication cost. Let's see the techniques which guide how the system follows toward its goal. There is an opportunity to select the best cryptographic algorithm which is preferable to NFC tag, based on this we have chosen a Public Key Cryptographic (PKC) algorithm.

a. At the first movement each organization should be apply for registration into third trusted party
b. The third trusted party assuring the legitimacy of an applicant organization and if they are legitimate organization then it provides a security key (private key) for next time of secure communication.
c. Before sending information towards the trusted party, the registered organization should be encrypting the required users' certificate related information by its own secret key.
d. After received encrypted information and server's ID the trusted party to be search public key of sender's organization according to sender's ID. Then after finding the key it try to decrypt the receipt messages finally stored the required information into its database and randomly generate a key to encrypt the stored information of receipt information let it considered as
$M1=E_{RK}$(Message) and compute M2 by encrypting M1 using trusted party's private key.
$M2=E_{SK}$(RK) then send
M3={M1,M2,Tag_decryption_Key}

e. Now, the sender organization is received the reply message M3. Then write all received information on the tag
f. Configure the reader by third trusted party through recording Tag_encryption_key, trusted party public key. Finally, The organization upload the application on their well-known popular website for available to download by any users.
g. The reader perform the following activities
   1. Send the reading request to the tag
   2. The tag generate random number and send it to the reader
   3. Then the reader encrypt that number and send it back
   4. The tag decrypted the received encrypted number and check that the result is match with the number or not if so then send M1 after M2
   5. The reader decrypt M2 by trusted party's decryption key
   6. Now the reader have messages encrypted key as a result
   7. Then decrypt the message by newly founded key
   8. Finally, it will display the screened information as well as originality notification message on user's cell phone to help the user making result comparison with printed paper's content

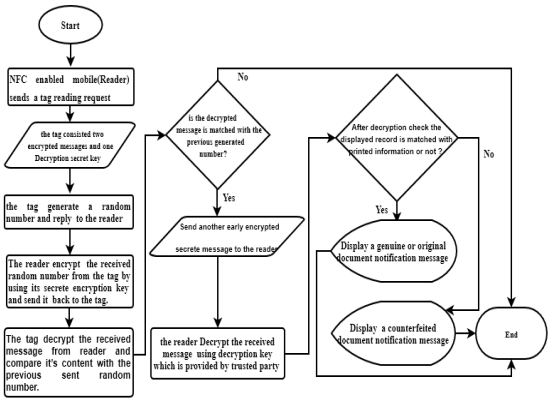

Fig 2:-*Document verification dataflow at end users' environment*

As mentioned below, there are three basic categories of public Key cryptography:

1. **Encryption/decryption (secrecy)** – sender encrypts the message with recipient's public key.
2. **Digital signatures (authentication & data integrity)** – sender encrypts message with his/her private key.
3. **Key exchange (of session keys)** – several approaches, using one or two private keys.

Based The Rivest, Adi Shamir, and Leonard Adleman(RSA) public-key encryption scheme pair of private and public keys can be generated. Let n = pq, where p and q are two large prime numbers. Let M = C = Zn. Pick a number e relatively prime to φ(n) and calculate a number d such that

ed = 1 mod φ(n). The public key is the two numbers (n,e) and the (public) encryption transformation E(M) is
$E(M) = M^e \bmod n$.
The secret key is the number d (as well as p, q and φ(n)) and the secret decryption transformation D(C) is

$$D(C) = C^d \bmod n.$$

Verify that decrypting a cipher text returns the encrypted plaintext.

$$D(C) = C^d = (M^e)^d = M^{ed} \bmod n.$$

Now we note that ed = 1 mod φ(n), which means that we can write
ed = 1 + t · φ(n),
for some integer t. we can continue

$$D(C) = M^{ed} = M(^{1+t\cdot\varphi(n)}) = M * M^{t\cdot\varphi(n)} \bmod n.$$

From Euler's Mathematical formula can drive
$x^{\varphi(n)} = 1$ for any $x \in Z^*_n$. So assuming that M is invertible we have $D(C) = M*M^{t\cdot\varphi(n)}$
= M * 1 mod n. However, for better security strength we are proposed to use the integration of all the above mentioned categories,

b. Hardware and software Resources

1. **Software**
   - i. **Android SQLite**: - This built-in database is being provided by the operating system itself
   - ii. **Java**:- We use to develop the system with android platform
   - iii. **PHP with MySQL database**: This is an external database which is useful to develop the system for serving at organizations side. Whereas the built-in SQLite is useful for developing the code at readers' side.
   - iv. **Apache**
   - v. **NS2 simulator**
   - vi. **XAMP**

2. **Hardware**
   - i. NFC Tag
   - ii. NFC enabled mobile
   - iii. Sample certificate

VI. Result Analysis

1. Security Analysis

In this section, we give the security analysis of our security scheme protocol. We will show that our protocol efficiently achieves high security against the most common attacks. It is able to overcome weaknesses "Secure Authentication Scheme for Medicine Anti-counterfeiting System in IoT Environment" and "Development of Vegetable Traceability System Based on RFID and Barcode Technology", protocols and is more adequate for our applications.

S1: Mutual Authentication

A bilateral authentication is necessary and decisive when each component involved in a given transaction has to check the identity of the other. Without mutual authentication, the tag or reader identity's usurpation becomes possible. Consequently the presence of this security mechanism could highlight and improve care services and certificate owners' safety. The proposed protocol provides mutual authentication between the different communicating parties.

S2: Data Integrity

The data integrity property is very important in our proposed system context. Since, preserving the integrity and completeness of the healthcare data may enormously enhance organizations safety, increase efficiency and reduce errors and adverse incidents that could occur as a result of altered data and information. The data integrity property is of primary importance in our context. In our proposed protocol, we have used the Public key Cryptographic value of the transfer encrypted data by trusted organization's secret key technique to verify the data integrity.

S3: Scalability and Efficiency

The scalability is considered as one of desirable features in an NFC system. This property allows avoiding a computational workload of the searching process proportional to the number of tags of the system. Thus, if this computational searching cost increases linearly with the number of tags in the DB, the system is not scalable. In our proposed protocol we use the pseudonym technique, where each tag identifier IDkj matches only one NFC tag in database. So, the back-end server takes IDkj as an index to get the corresponding data records in database. Consequently, no exhaustive search is required for the tag identification. As a result, the proposed protocol ensures a high efficiency in the tag identification process.

S4: Replay Attack Resistance

A replay attack is an offensive action where an adversary could imitate the legitimate tag or server by reusing the messages obtained from previous sessions. Via intercepting previous messages, an adversary may replay these messages to pass the authentication process of the NFC system. In the

proposed protocol, messages are freshly generated using the temporary random numbers Rr by the tag, and encrypt it using secret key of reader. In addition, our system works in an offline environment among between reader and tag, which allow guaranteeing a protection against the replay attacks.

Table 1*Functionality and security issues comparisons against some related protocols*

Features Protocols	Development of Vegetable Traceability System Based on RFID and Barcode Technology	An NFC Based Consumer-Level Counterfeit Detection Framework	Secure Authentication Scheme for Medicine Anti-counterfeiting System in IoT Environment	Our proposed protocol
S1	No	No	Yes	Yes
S2	No	No	No	Yes
S3	No	Yes	Yes	Yes
S4	No	Yes	Yes	Yes
S5	No	No	No	Yes
S6	Yes	Yes	No	Yes

S1: mutual authentication
S2: data integrity
S3: scalability and efficiency
S4: Replay attack resistance
S5: Less computation and communication cost
S6: Trustfulness

2. Performance analysis

The detailed computation cost comparisons with some related works in the literature presented results and mainly in "Secure Authentication Scheme for Medicine Anti-counterfeiting System in IoT Environment" protocol. We can say that our proposed protocol does not require an extra computational workload to support the introduced security enhancements that guarantee new functionalities such as integrity, efficiency and authorization.

VII. ACKNOWLEDGEMENTS

At the first glance we would like to thank our almighty God. At the second place thanks for our parents, they provide moral supports for this work. Next, we would like to thank some of our friends and colleagues, they live in here as well as Parule University, about their collaboration to work and share ideas with us and they help us by purchasing inaccessible supportive materials such software and tags. Finally, we would like to thank our project coordinator.

VIII. CONCLUSION

Almost all of the reviewed papers are designed the security schemes based on RFID tag security techniques however, this is not accessible at everywhere because the requirement of physical RFID reader device so this is not that much affordable to all users, and the remain papers are designed the scheme using NFC technology which is read by the NFC enabled mobile this is better solution than the previous but those have also un trustful because lack of third trusted authorized party in addition to that not yet develop a security scheme for fake documents prevention techniques.

Now, we proposed to design the security scheme that eliminates the limitation of previous papers using NFC technology with low computation and communication costs of tag compatibility cryptographic algorithm and design a new scheme for highest valuable certificates prevention and protection from releasing fake copies of them into the market.

Generally, our proposed scheme is designed based on Public Key Cryptographic algorithm and successfully detect counterfeited certificates in two phases of communication along with third trusted governmental authorized party. These are; a communicationbetween applicantorganizationand trusted partyvia a secured web-based system. In the other hand an offline communication between NFC tag embedded certificate and NFC reader application on NFC enabled smartphone.

REFERENCES

[1].C.Wenxue,H.Qinghao,O.Zhirong,P.Zhe,Z.Guanxiang,"Development of vegetable traceability system based on RFID and Barcode technology." In *Service Systems and Service Management (ICSSSM), 2014 11th International Conference on*, pp. 1-5. IEEE, 2014.

[2].M.Taolin, H.Zhang, J.Qian, S.Liu, X.Zhang, and X.Ma, "The Design of Brand Cosmetics Anti-counterfeiting System Based on RFID Technology." In *Network and Information Systems for Computers (ICNISC), 2015 International Conference on*, pp. 184-189. IEEE, 2015.

[3]. S.Zhicai, A lightweight RFID authentication protocol based on Rabin cryptosystem. *International Journal of Emerging Trends & Technology in computer science,*vol.5,Issue 2,April 2016.

[4]. S.M.Qasim, Z.Bilal, and C.D.Walter,"An NFC based consumer level counterfeit detection framework." In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*, pp. 135-142. IEEE, 2013.

[5]. B.Xu, L.Zhang, and X.P.Tan, "Research of RFID certification security protocol based on hash function and DES algorithm." *Journal of Networks* 8, no. 10 (2013): 2368-2376.

[6]. B.Mustapha, M.Djeddou, and K.Drouiche , "Security Analysis and Enhancement of the Most Recent RFID Authentication Protocol for Telecare Medicine Information System." *Wireless Personal Communications* 96, no. 4 (2017): 6221-6238.

[7]. W.H.Lee, C.M.Chou, and S.W.Wang, "An NFC Anti-Counterfeiting Framework for ID Verification and Image Protection." *Mobile Networks and Applications* 21, no. 4 (2016): 646-655.

[8]. R. Aparna, V.Ravi,"Security in RFID based smart retail system." In *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, pp. 587-592.IEEE, 2016.

[9].A.Goswami, A. K.Das and V.Odelu, "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms." *IEEE Transactions on Consumer Electronics* 62, no. 1 (2016): 30-38.

[10]. A.Al-Ghaiheb,A.K. Das, A.Vasilakos, M.K. Khan, N.Kumar, and W.Mohammad, "Secure Authentication Scheme for Medicine Anti-counterfeiting System in IoT Environment." *IEEE Internet of Things Journal* (2017).

[11].G.Lijun, L.Zhang, and M.Ma. "Low Cost RFID Security Protocol Based on Rabin Symmetric Encryption Algorithm." *Wireless Personal Communications* (2017): 1-14.

[12]. W.Ying. "Design of an anti-counterfeiting system based on SMS." In *Granular Computing, 2009, GRC'09. IEEE International Conference on*, pp. 572-575. IEEE, 2009.

[13].Q.Chang. "RFID Applications in Agriculture and the Issues [J]." *Radio Frequency Identification Technologies and Applications* 6 (2008): 014.

[14].H.H.Cheung, S.H.Choi,"Implementation issues in RFID-based anti-counterfeiting systems." *Computers in Industry* 62, no. 7 (2011): 708-718.

[15].L.Jiqiang. "Related-key rectangle attack on 36 rounds of the XTEA block cipher." *International Journal of Information Security* 8, no. 1 (2009): 1-11.

[16]. L.Ticyan, and G.Wang. "Security analysis of two ultra-lightweight RFID authentication protocols." *New approaches for security, privacy and trust in complex environments* (2007): 109-120.

[17]. L.Y.Xiao, H.S.Shi, and S.P.Zhang. "An energy-efficient MAC protocol for wireless sensor network." In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 4, pp. V4-619. IEEE, 2010.