Journal of Engineering and Applied Sciences 12 (22): 6006-6012, 2017
ISSN: 1816-949X

Two Different Authentication Protocol for RFID Credit Card Security

Rohit Sharma, Pankaj Singh and Abhishek Singhal
Department of Electronics, SRM University, Ghaziabad, India

Abstract: RFID (radio recurrence recognizable proof) is a remote programmed ID innovation that utilizations radio signs to distinguish an item, creature or individual. A RFID framework contains of RF labels, label perusers and backend server. A RFID tag is a little microchip with a reception apparatus, holding an extraordinary ID and other data. The data can be sent over radio recurrence to RFID perusers and handled by a back-end database. With the critical points of interest of RFID innovation, RFID is by and large bit by bit embraced and created in a wide territory of uses including inventory network administration retailing, get to control framework, creature recognizable proof and human services. Through the programmed information gathering, RFID innovation can accomplish more noteworthy perceivability and item speed crosswise over supply chains, proficient stock administration, simpler item following and observing, diminished item falsifying and robbery and highly decreased work cost. With the broad utilization of this innovation, the presence of the security and protection issues turn out to be more noticeable which must be fathomed. The RFID security hazard is about secrecy, honesty, accessibility and legitimacy. Classification is a security hazard as correspondences amongst labels and perusers are uncovered or spying and activity examination which may permit a man-in-the-center assault. Here we examine to significant convention acquainted with secure the RFID transmission in the middle of tag and peruser. To start with convention talks about the approach containing the utilization of an irregular piece generator alongside a solid encryption plot. What's more, second approach included a profoundly complex scientific process for securing the information amongst tag and peruser.

Key words: RFID security, sensor network, Euclidean parameters, transmission, administration, approach

INTRODUCTION

A RFID framework involves label, peruser and backend server as its principle parts. Labels, the essential building piece of RFID, comprise of a chip, reception apparatus and a specific measure of computational and capacity abilities. A peruser inquiries tag to acquire label substance and sends the encoded data got from the tag to the backend server for checking the authenticity of the tag. The backend server contains a nearby database and a few processors (Li *et al*., 2010). The labels, the transponders are questioned by perusers through a remote unreliable channel. The fundamental channel between a peruser and the backend server might be wired or remote and is secured1 as appeared in Fig. 1. The labels might be delegated uninvolved, semi latent and dynamic as per the way they are fueled. In this study, we have considered latent labels that require no inner power yet are fueled from the radio flag sent from the peruser while they question the tag.

As the latent labels have low stockpiling and low computational abilities, they experience the ill effects of numerous security defects. Because of the restrictions on capacity, RFID verification conventions utilize minimal

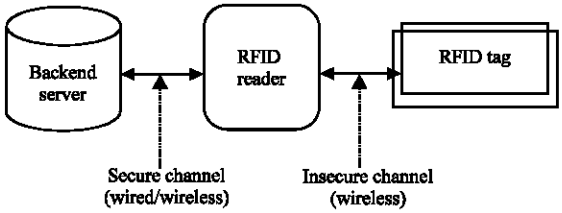

Fig. 1: Interaction between tag, reader and backend server

effort cryptographic primitives like bitwise operations, pseudorandom number generators, hash capacities and so on, here, we talk about to significant convention acquainted with secure the RFID transmission in the middle of tag and peruser.

In the first place convention examine the approach containing the utilization of an arbitrary piece generator alongside a solid encryption plot. What's more, second approach included a very perplexing scientific process for securing the information amongst tag and peruser (Fu *et al*., 2010).

Literature review: A few validation plans have been proposed for giving security in RFID frameworks. Here,

Corresponding Author: Rohit Sharma, Department of Electronics, SRM University, Ghaziabad, India

we give a short audit of a few conventions. Albert utilize three stages for verification: introduction, recognizable proof (synchronized and desynchronised) and refreshing stage. This convention utilizes the PRNGs to deliver an unusual pseudo-irregular arrangement. In Fu an adaptable pseudo irregular based shared verification plan is suggested that includes encryption in view of symmetric key cryptography, arbitrary number generators and hash work. It utilizes an assumed name of label ID, refreshes it in each validation and requires EEPROM memory for this reason. Min examine a dynamic token based verification plot. This convention gives secrecy and verification through arbitrary instatemare refreshed powerfully using the base token and base pointer cluster utilized. This plan however, requires more stockpiling in the tag for these clusters and updates. It doesn't bolster common verification and inclined to desynchronization assault. In the plan of Gui a hash work based keyed encryption is utilized for validation and proprietorship exchange. This encryption work partitions the labels into a few gatherings and grouping of the label requires to be checked. Irfan proposed a confirmation conspire in light of cryptographic hash chain. However, utilizing the hash recursively more circumstances requires more stockpiling and calculations. The convention proposed by Chang *et al*. (2009) is an enhanced adaptation to the convention by Venkatraman. They have distinguished some protection worries in the Venkatraman protocol and proposed another plan without the RFID middle ware. In the Chang *et al*. (2009) a verification procedure is completed by considering the past session end. Rahman talked about a convention in view of PRNG yet it expect that peruser has every one of the privileged insights before verification handle begins and restricts its applications. Li give a validation plan that utilizations pseudo-arbitrary generators at peruser side and performs ID and key refreshing on each effective confirmation. Be that as it may, this plan is not secure against the traceability assault.

MATERIALS AND METHODS

Sensor network method for rfid system: In the earlier years an essential change for PC frameworks happened: the rising of direct device to-device or machine-to-machine correspondence within general PC frameworks. An essential issue for machine-to-machine correspondence is that the surge of information complexities extensively from that in present-day PC frameworks. Instead of a significant stream from central servers to clients at the edge of the framework, the rule data stream for RFID and sensor framework structures is from various contraptions at the edge of the framework towards two or three central servers (Fu *et al*., 2010). In both systems, sensors or RFID perusers perceive certain events and forward the relating information to some business application on a central server.

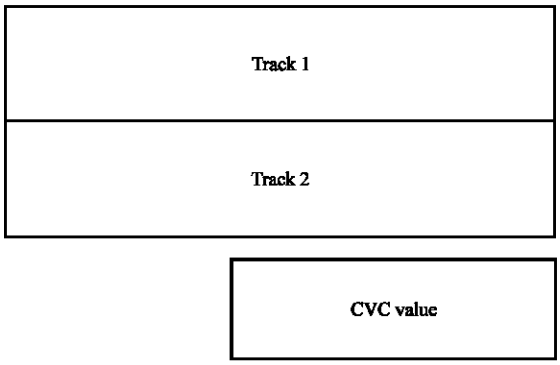

Fig. 2: RFID credit card data format

For machine to machine correspondence (RFID to sensors), we furthermore require another programming building outline.

Card header format: Further also we have to change the header format of RFID credit card for this model. As in a simple credit card (Fig. 2), this information's (track 1, 2 and CVC value) are used during transaction with POS terminals (Sharma *et al*., 2015a-c). Here, we try to show the output stream of a simple card.

Serial yield from a business peruser after a RF exchange with a card from backer A:

Dxxxxxx5251xxxxxx^DOE/JANE^080620
20000000000000000000000000929000000 (1)
Xxxxxx5251xxxxxx=08062020000092900000

Equation 1 exhibits a case of this serial yield which consolidates all the standard parts of an ISO 7813 magstripe. The important line addresses track 1. The start sentinel B is trailed by the fundamental record number. Taking after the field-separator character, the cardholder name appears, trailed by another field-separator and an "additional data" field. This field joins not only the card close date (for this circumstance 06/2009), furthermore a long arrangement of digits (Chen and Chen, 2015; Dass and Om, 2016).

The second line addresses standard track 2 data which is, all things considered, similar to the track 1 data. Track 2 does not contain the cardholder name and contains less space for prohibitive information (Sharma *et al*., 2015a-c).

The primary code, called CVC1 or CVV1 is encoded on track 2 of the alluring stripe of the card and used for card exhibit trades. The inspiration driving the code is to watch that a portion card is truly in the hand of the merchant. This code is thus, recouped when the alluring stripe of a card is swiped on a state of scale (card display) gadget and is affirmed by the benefactor. An imprisonment is that if the entire card has been replicated and the alluring stripe copied, then the code is still honest to goodness (Sharma *et al*., 2015a-c; Gui and Zhang, 2013).

The second code and the most alluded to, is CVV2 or CVC2. This code is every now and again searched for by brokers for card not indicates trades happening by means of mail or fax or through telephone or internet. In a couple of countries in Western Europe, card sponsor oblige a broker to get the code when the cardholder is not present in individual.

Proposed model is worry with each one of the three information's. CVC quality reacts as a covered worth for customers. It simply can be perused by the RFID peruser (Sharma *et al*., 2015a-c).

Model architecture and overview: A couple conditions and essentials need to look for this model as RFID peruser deactivated until it gets any summon from second sensor (Sharma *et al*., 2015a-c). At first RF sensor is used to track the region of RFID card under its range. As it found the region of any RFID Visa, in a flash RFID card respond back with its CVC regard. Gotten CVC worth will be sent to second sensor. Second sensor will serially send CVC worth and sporadic piece (from discretionary bits generator) to the RFID peruser (Sharma *et al*., 2015a-c).

Gotten unpredictable bits will be secured by the peruser and a copy will be sent to the RFID card. In second step, RFID peruser endeavoring to focus the track information of customer with the CVC regard by sending it to base station.

To comprehend the procedure quickly, investigate the proposed conspire diagram given beneath. It is unmistakably clarified in Fig. 3 that the procedure is totally secure against the assortment of enemy assaults (Sharma *et al*., 2015a).

A high breaking point encryption must be performed on both sides (peruser and card). Encoding result from both sides must be same for working up an association (Sharma *et al*., 2015b).

High farthest point encryption methodology must be introduced for the proposed display. In next parts, I proposed some new encryption plots that check the security of trade between RFID card and RFID peruser (Sharma *et al*., 2015c).

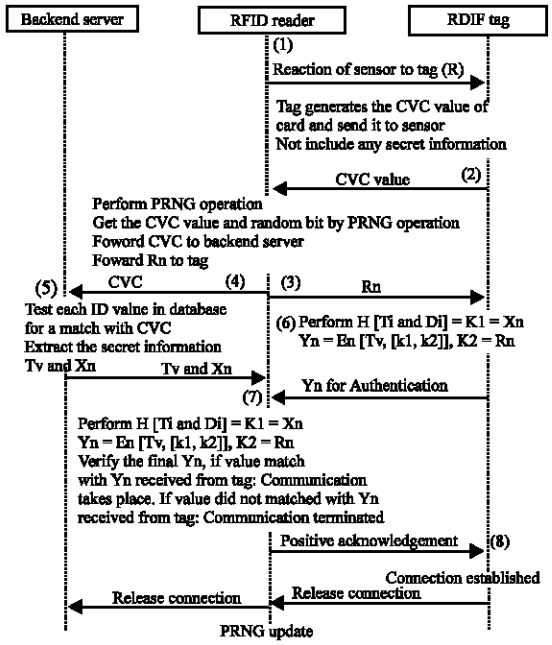

Fig. 3: Proposed scheme overview

RESULTS AND DISCUSSION

Comparative analysis

Security analysis: Table 1 analyze security parts of our plan alongside some current verification plans against the most normally happening assaults in RFID frameworks (Sharma *et al*., 2015a-c).

Obscurity of tag: Not sharing the data publically amid the transmission.

Replay assault resistance: Adversary can't utilize the recorded information for unapproved get to.

De synchronization resistance: Adversary can't change the information inside the tag.

Classification and respectability: Secret data in totally private.

Shared authentication: Use the present information to separate the data about future information. For our situation, it is difficult undertaking on the grounds that the information transmitted from tag to peruser is totally arbitrary in nature (Fu *et al*., 2010).

Traceability resistance: Not simple to record the information and concentrate the data. For our situation, it is difficult assignment in light of the fact that the information transmitted from tag to peruser is totally irregular in nature.

Table 1: Security analysis of proposed scheme

Variables	Fu *et al.* (2010)	Gui and Zhang (2013)	Chang *et al.* (2009)	Li *et al.* (2010)	Chen and Chen (2015)	Dass and Om (2016)	Ours
Anonymity of tag	Y	Y	Y	Y	Y	N	Y
Resistivity replay attack	Y	Y	Y	Y	Y	Y	Y
De synchronization resistance	N	N	N	Y	N	Y	Y
Confidentiality and integrity	Y	Y	Y	Y	Y	Y	Y
Mutual authentication	N	Y	Y	Y	N	Y	Y
Traceability resistance	N	Y	Y	N	Y	Y	Y
Forward secrecy	N	Y	Y	N	Y	Y	Y
MITM attack resistance	Y	Y	Y	Y	Y	Y	Y
Master key attack	Y	N	N	N	N	N	Y
DoS attack resistance	N	N	N	Y	N	N	Y

Y-Satisfy; N-Not

Table 2: Operation cost analysis of proposed scheme

Variables	No. of communications with tag	Computation cost at tag
Li *et al.* (2010)	3	$2T_X+1T_R+4T_H$
Dass and Om (2016)	3	$1T_R+1T_X+3T_F+2T_H$
Chang *et al.* (2010)	3	$4T_H+11T_X+2T_R$
Fu *et al.* (2010)	4	$2T_R+2T_X+4T_H$
Chen and Chen (2015)	3	(a*m+b*n) $T_X+1T_S+1T_F+2T_H$
Gui and Zhang (2013)	4	$2T_R+1T_F+2T_X+3T_H$
Ours	5	$1T_R+1T_H+1E_N$

T_X: Cost of XOR operation; T_H: Cost of Hash function; T_R: Cost of Random number generation operation; T_F: Cost of Flip operation; T_S: Cost of circular shift operation; T_P: Cost of PRNG operation; E_n: Cost of encryption operation; m and n represents the lengths of two base arrays that store a-bit base tokens and b-bit base indicators

Forward mystery: Present information is not valuable for foe for making expectation about future data.

MITM attack resistance: It resembles listening in, enemy record the correspondence amongst card and peruser for removing the mystery data.

Ace key attack: Adversary apply an arrangement of keys for the extraction of data from recorded information. For our situation, we are utilizing a solid encryption conspire so it is unrealistic to concentrate mystery data (Dass and Om, 2016).

DoS attack resistance: Adversary obstruct some measure of data being transmit from tag to peruser. To maintain a strategic distance from this insufficiency, we played out a PRNG refresh operation after each exchange.

Operation cost analysis: Here, we discuss execution examination of our proposed modular to the extent operations included, stockpiling and correspondence overhead. The cost of operations of different traditions/contrives nearby our arrangement is showed up in Table 2. The quantity of correspondences made with the tag is also said in this Table 2 (Li *et al.*, 2010).

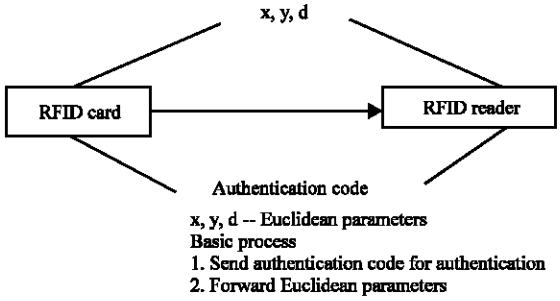

Fig. 4: Proposed transaction model

It is clear from Table 1 that our proposed scheme does not increase the cost of tag, we are not repeating any operation again and again so it not requires any additional storage for updating the value at tag side. And it also makes secure the tag from de synchronization and DOS attack (Chen and Chen, 2015).

Euclidean parameters method along with polynomial arithmetic: RFID Card are creating in noticeable quality in light of the way that they permit contactless portion trades which are brisk, straightforward can be more strong than magstripe trades and require simply physical region (rather than physical contact) between the card and the peruser. These same components, regardless are in like manner the introduce for our stress over security and assurance vulnerabilities (Sharma and Singh, 2015). Standard card oblige that a component have visual get to or coordinate physical contact remembering the ultimate objective to get information from the card, for instance, the cardholder's name and the card number (Sharma and Singh, 2015; Sharma *et al.*, 2015a-c).

To complete the trade, RFID card use a data configuration (Fig. 4 and 5) which contain CVC esteem, track 1 and 2 information. CVC esteem is a card check code and track information contains the information about the card holder (Sharma *et al.*, 2015a-c).

Table 3: Security analysis of proposed scheme

Variables	Fu *et al.* (2010)	Gui and Zhang (2013)	Chang *et al.* (2009)	Li *et al.* (2010)	Chen and Chen (2015)	Dass and Om (2016)	Ours
Anonymity of tag	Y	Y	Y	Y	Y	N	Y
Resistivity replay attack	Y	Y	Y	Y	Y	Y	Y
De synchronization resistance	N	N	N	Y	N	Y	Y
Confidentiality and integrity	Y	Y	Y	Y	Y	Y	Y
Mutual authentication	N	Y	Y	Y	N	Y	Y
Traceability resistance	N	Y	Y	N	Y	Y	Y
Forward secrecy	N	Y	Y	N	Y	Y	Y
MITM attack resistance	Y	Y	Y	Y	Y	Y	Y
Master key attack	Y	N	N	N	N	N	Y
Dos attack resistance	N	N	N	Y	N	N	Y

Y-Satisfy; N-Not

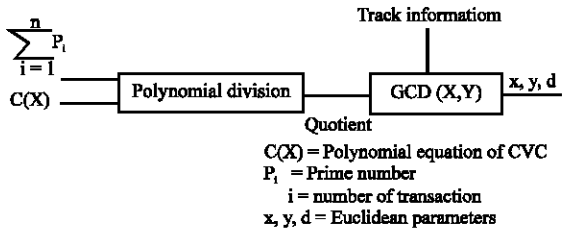

Fig. 5: Cryptosystem model

For our cryptosystem, CVC esteem ought not be engraved on the card (must be concealed inside the card). In this study, we performed polynomial arithmetic close by Euclidean operation on RFID card data setup to make trade secured. The upside of the count is that simply couple of Euclidean parameters will send to the peruser at the spot of finish process (Sharma and Singh, 2015).

x, y and d are the Euclidean parameters that made by a numerical strategy. Introductory a validation code must transmit to the peruser. Additionally trade method will start after the verification (Fig. 5). Peruser need to focus the plainest or information by the got Euclidean parameters (Sharma and Singh, 2015).

Proposed cryptosystem for RFID security: Cryptography is utilized as a part of e-trade for validation and secure correspondence. The most broadly utilized cryptosystems RSA and ECC (Elliptic Curve Cryptosystems) are taking into account the issue of whole number factorization and discrete logarithm individually (Sharma and Singh, 2015).

To grow the multifaceted nature and upgrade the security, we performed polynomial number juggling operation between the card CVC esteem (to be concealed inside the card) and "prime numbers" delivered by prime number generator (Fig. 6).

Polynomial division must be performed between polynomial numerical articulation of CVC esteem and prime number. Encourage for Euclidean parameters, the remainder and track information will be used as data for Greatest Common Divisor (Sharma *et al.*, 2015a).

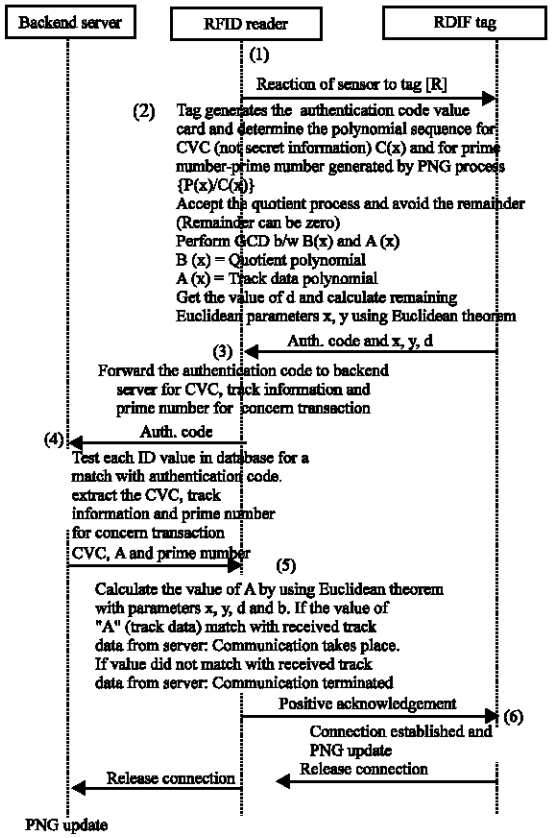

Fig. 6: Proposed scheme overview

A relative definition is the going with: GCD [A(X), B(X)] is the polynomial of most prominent degree that segments both A(X) and B(X). We can change the Euclidean estimation to enroll the best normal divisor of two polynomials (Sharma and Singh, 2015).

To comprehend the procedure quickly, investigate the proposed conspire outline given underneath. It is unmistakably clarified in Fig. 7, that the procedure is totally secure against the assortment of foe assaults.

Here validation is also a bit of decoding. In any case transmitter needs to complete the confirmation of RFID card with the help of verification code (Fig. 7). Transmitter

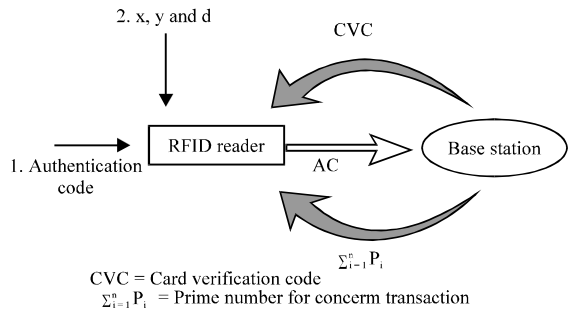

Fig. 7: Decryption model

Table 4: Operation cost analysis of proposed scheme

Variables	No. of communications with tag	Computation cost at tag
Li *et al.* (2010)	3	$2T_X+1T_R+4T_H$
Dass and Om (2016)	3	$1T_R+1T_X+3T_P+2T_H$
Chang *et al.* (2010)	3	$4T_H+11T_X+2T_R$
Fu *et al.* (2010)	4	$2T_R+2T_X+4T_H$
Chen and Chen (2015)	3	(a*m+b*n) $T_X+1T_S+1T_F+2T_H$
Gui and Zhang (2013)	4	$2T_R+1T_F+2T_X+3T_H$
Ours	3	$1T_P+1T_{PNG}+1T_D+1T_{GCD}+1T_{EPC}$

T_X: Cost of XOR operation; T_D: Division operation; T_H: Cost of Hash function; T_R: Cost of Random number generation operation; T_F: Cost of Flip operation; T_S: Cost of circular Shift operation; T_P: Cost of PRNG operation; T_{GCD}: Greatest Common Divisor; E_n: Cost of Encryption operation; T_{EPC}: Euclidean Parameter Calculation; m and n speaks to the lengths of two base exhibits that store somewhat base tokens and b-bit base markers

will forward the confirmation code to the base station. After the total affirmation, base station sends the CVC estimation of card and prime number for concern exchange. RFID peruser will make the polynomial sort of CVC and concern prime number to execute the estimation of Quotient B(X) (Sharma *et al.*, 2015; Gui and Zhang, 2013):

$$C(X) = X^4+X^3+1$$

$$\sum_{i=1}^{n} P_i \; i=1,2,3,4,\ldots,n$$

Comparative analysis

Security analysis: In Table 3, we analyze security parts of our plan alongside some current verification plans against the most normally happening assaults in RFID frameworks (Sharma *et al.*, 2015a-c).

Operation cost analysis: Here, we discuss execution examination of our proposed modular to the extent operations included, stockpiling and correspondence overhead. The cost of operations of different traditions/schemes close by our arrangement is showed up in Table 4. The quantity of correspondences made with the tag is furthermore said in Table 4 (Chen and Chen, 2015).

It is clear from Table 4 that our proposed conspire does not build the cost of label, we are not rehashing any operation and again so it not requires any extra stockpiling for refreshing the incentive at label side. What's more, it additionally makes secure the tag from de synchronization and DOS assault (Sharma *et al.*, 2015).

CONCLUSION

These proposed models are worry with the trade security between RFID card and peruser. To upgrade the security, we go without sharing the information amidst peruser and card. Peruser will execute the information by using polynomial number juggling nearby Euclidean parameters. In our cryptosystem the key is the blend of some polynomial division, prime numbers, CVC regard and most prominent regular divisor.

The yield of prime number generator will change after each trade; suggests for each and every trade, we have a substitute estimation of key. This property of our cryptosystem will perplex the foe. Additionally, other property of our cryptosystem is; simply couple of Euclidean parameters have partaken amidst transmitter and recipient. It is not straightforward for enemy to execute the estimation of "a" and "b" by x, y and d parameters in light of the way that we can have unlimited amounts of blend of "a" and "b" for a similar estimation of x, y and d.

REFERENCES

Chang, A.Y., D.R. Tsai, C.L. Tsai and Y.J. Lin, 2009. An improved certificate mechanism for transactions using radio frequency identification enabled mobile phone. Proceedings of the 43rd Annual International Carnahan Conference on Security Technology, October 5-8, 2009, IEEE, Zurich, Switzerland, ISBN:978-1-4244-4169-3, pp: 36-40.

Chen, M. and S. Chen, 2015. An efficient anonymous authentication protocol for RFID systems using dynamic tokens. Proceedings of the 2015 IEEE 35th International Conference on Distributed Computing Systems, June 29-July2, 2015, IEEE, Columbus, Ohio, ISBN:978-1-4673-7214-5, pp: 756-757.

Dass, P. and H. Om, 2016. A secure authentication scheme for RFID systems. Procedia Comput. Sci., 78: 100-106.

Fu, J., C. Wu, X. Chen, R. Fan and L. Ping, 2010. Scalable pseudo random RFID private mutual authentication. Proceedings of the 2010 2nd International Conference on Computer Engineering and Technology Vol. 7, April 16-18, 2010, IEEE, Chengdu, China, ISBN:978-1-4244-6349-7, pp: 497-500.

Gui, Y.Q. and J. Zhang, 2013. A new authentication rfid protocol with ownership transfer. Proceedings of the 2013 International Conference on ICT Convergence, October 14-16, 2013, IEEE, Jeju, South Korea, ISBN:978-1-4799-0698-7, pp: 359-364.

Li, J., Y. Wang, B. Jiao and Y. Xu, 2010. An authentication protocol for secure and efficient RFID communication. Proceedings of the 2010 International Conference on Logistics Systems and Intelligent Management Vol. 3, January 9-10, 2010, IEEE, Harbin, China, ISBN:978-1-4244-7330-4, pp: 1648-1651.

Sharma, R. and P.K. Singh, 2015. The simulation and analysis of RC4 and 3DES algorithm for data encryption in RFID credit card. Intl. J. Appl. Eng. Res., 10: 4265-4273.

Sharma, R., A.K. Agarwal and P.K. Singh, 2015b. Advancement in RFID security by proposed framework utilizing Random bit generator and sensor network. Intl. J. Adv. Comput. Res., 5: 321-326.

Sharma, R., A.K. Agarwal and P.K. Singh, 2015c. Transaction security in RFID credit card by polynomial arithmetic along with euclidean parameters. Intl. J. Eng. Technol., 7: 1194-1199.

Sharma, R., K.A., Anuj and P.K. Singh, 2015a. Data security by (Information XOR Image) along with high capacity encryption to overcome steganography. Intl. J. Comput. Intell. Res., 11: 27-36.