COMPARATIVE STUDY OF TDES AND AES CRYPTOGRAPHIC ALGORITHM IN CASHLESS TRANSACTIONS

Abhishek

Abstract— In trendy day's use of cashless/digital payments is increasing day by day thanks to its easy service and completely different modes of transactions available in the market. Due to increase in the cashless/digital transaction the question arises is how secure the online payments system is. To answer this question there is need of cryptography or information security. Derived unique key per transaction is a key management scheme which generates set of secure unique keys from combination of super secret key and device's serial number one of which is used per transaction. If any derived key is compromised, transaction data is still protected since next keys cannot be determined easily. In cryptography we rewrite information in unintelligible form called as cipher text before sending it using encryption algorithms with the help of keys and decode/decrypt the information on receiving, most typically used cryptographic algorithms are AES and DES. Objective of this paper is to review cryptographic algorithms and their implementation using DUKPT, especially AES and TDES and their operating in cashless/digital payments systems, and compare these algorithms with regard to the security level, complexity, memory requirement and other aspects.

Index Terms-AES, BDK, Cryptography, DES, Digital Transaction, DUKPT, key, Security.

1 Introduction

In modern days, cashless/digital transaction or electronic transaction have been widely used in place of cash/money based commercial transactions, that makes it easy for a user to pay through alternative ways of e-transaction e.g. Credit/debit cards, internet banking, mobile banking, UPI etc.

In most of the cases it is observed that there are number of attacks on cashless based transactions by the attacker. The most important question that arises from these kinds of attacks is how secure the payments system is. To answer this question, cryptography or any security technique plays a crucial role. Cryptography is the science and art of reworking original messages into an unreadable form to secure the info. [4]

Derived unique key per transaction (DUKPT) is a key management scheme which generates set of secure unique keys from combination of super secret key and device's serial number one of which is used per transaction. If any derived key is compromised, transaction data is still protected since next keys cannot be determined easily; it is described in ANSI X9.24 [6]

This scheme allows the encryption to be moved away from devices that hold shared secret. The encryption is done with a unique derived key. It is typically used to encrypt the PIN or card information of user acquired by point of sale (POS) devices.

The basic reason of threat in on-line/digital or electronic transaction is unauthorized use of personal advantages. Use of cryptographic techniques is one of the popular ways to avoid such unauthorized attacks and to prevent insecure permissions, and other possible threats. Some of the Popular cryptographic algorithms like DES, TDES and AES provides high level of security to the system that makes it very troublesome or not possible for a attacker to gain access to the system and steal any vital information. DES uses 64 bits plain text and 56 bits key(additional eight bits for error checking or alternative use) to encrypt the original plain text using some mathematical calculations,16 rounds of shift and xor operation to provide complex keys. Triple DES is doing the DES three times to make it more complex and effective against attacks. AES uses 128 bit plain text and 128,192,256 bit keys to encrypt the original plain text. [5]

By using combination of symmetric key encryption algorithms with the DUKPT key management scheme makes it highly secure and efficient for a payment system/device.

2 Literature Review

Eric brier and Thomas peyrin (conference 2010)[1]", Forward secure symmetric key derivation protocol using DUKPT", described about the DUKPT key encryption scheme and also provided improvements over the classical scheme.

Amal saha, Sugata sanyal (journal 2014) [2], "Applicability of DUKPT Key Management Scheme to Cloud Wallet and other Mobile Payments", authors discuss about the working of DUKPT scheme and its applicability in various payment systems.

In Paper [3] Saptarshi Mitra, Bappaditya Jana, and Jayanta Poray, "Implementation of a novel security technique using

- *Author name is Abhishek currently pursuing masters degree program in computer science and engineering in National Institute of Technology, Jalandhar, Punjab-144011, India, PH-9711058677, E-mail: aksmith95@gmail.com*

triple DES in cashless transaction"(conference 2017), gives overview of Triple DES algorithm and novel technique is used which is more secured than DES algorithm. Details are encrypted and then decrypted again at bank end.

In paper (journal 2019) [4], Vivek Kumar Singh, Shubham, "Security in Digital Payment", gives security concerns and proposed solutions, like encryption, digital signatures, firewall and secure protocols SSL and TLS and SET protocols

Paper [5] gives an performance evaluation of AES and DES in general use of encrypting and decrypting the plain text in terms of memory requirement, simulation time, avalanche effect and other aspects. The results deduced from the evaluations are, the memory requirement of AES is more than that of DES and simulation time is slightly higher for the AES algorithm as compared to DES, the avalanche effect is more in AES than in DES.

American National Standards Institute, ANSI X9.24-3:2017 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques (2009)[6], this scheme describes the secure key management scheme DUKPT and its applicability which is used to encrypt the payment data of a user on a Point of sale(POS) device by using unique key per transaction.

Paper [18], gives an illustrative view of the oldest symmetric block key encryption algorithm, DES the key elements of cryptography are plain text, key, encryption, cipher text and decryption.DES uses 64 bit plain text, and 56 bit key to generate round keys in all 16 rounds of shift and xor operation and finally the plain text is encrypted with the help of round keys to produce cipher text.

3 RESEARCH GAPS

After reviewing the literatures and previous work, the following gaps have been observed and work is done on those.

The following research gaps can be formulated as-

i) Proper secure encryption is not implemented Using secure key management.

ii) Encryption and decryption measures have not been compared for the digital payment system.

iii) Proper performance analysis is not done for any POS payment devices

This work tries to fill these gaps by analysing the encryption scheme and implementation to do performance analysis.

4 SECURITY AND CRYPTOGRAPHIC SIGNIFICANCE IN CASHLESS TRANSACTION

Cryptography is the science and art of changing original message (plain text) into a cipher text (unreadable text) by mathematical approach or alternative techniques using different cryptographic symmetric key and asymmetric key algorithms [7],[8],[13]. Security plays a vital role in cashless transactions due to the vulnerabilities present in transmission medium and components of cashless systems. [16]

Some protocols used for secure cashless transactions are:

SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer) and its successor TLS (Transport Layer security) protocols are used for establishing authenticated and encrypted links between networked pc systems.

HTTPS (Hypertext transfer protocol secure)

HTTPS (Hypertext transfer protocol secure) is the secured version of HTTP that is encrypted so as to send info between a web browser and a web site.

IPSec (IP Security)

IPSec provides authentication, Confidentiality and Integrity throughout secure transmission. IPSec is present within the network layer as a protocol with other important protocols like TCP, UDP etc.

Cryptography in cashless transaction verifies as well as preserves the five vital properties required in secure transmission of information from a sender to a receiver. The 5 important properties are [8],[13],[16]-

A. Confidentiality

Confidentiality refers to revelation or access of data solely to the authorized users only, and preventing any unauthorized access. User IDs and passwords helps achieving the goal of confidentiality.

B. Data integrity

Data integrity refers to the trustworthiness of the resource that the info a user is receiving is the original information from the authorized person solely. Data integrity protects the data from any modification throughout transmission; data integrity should not be compromised at any price.

C. Availability

Availability of the information and data resources, system ought to offer access to the resources required for process, storing or delivering the information whenever the user wants it. Because a system with resources not available at the time of need is marked as no system in any respect, thus availability of resources should be perpetually there.

D. Authentication

Authentication refers to the checking of identity of sender and receiver parties at each ends, whether they are legitimate/authentic or not.

E. Non repudiation

By non repudiation, the sender or receiver cannot deny that information is not sent or received by any party.

5 DUKPT AND ENCRYPTION IN DIGITAL PAYMENT

Derived unique key per transaction is a key management scheme which generates set of secure unique keys from aggregate of super secret key and key serial number of device, one of which is used per transaction. DUKPT is defined in ANSI X9.24. [2], [6]

ANSI standard defines DUKPT, X9.24-1 in 3DES mode, meaning DUKPT makes use of 3DES to generate Keys and it is called as 3DES-DUKPT. Another type is AES-DUKPT, which makes use of AES-ECB mode to generate key. Both have common inputs, Base derivation Key (BDK) and KSN with different size. For 3DES-DUKPT, BDK = sixteen bytes (always) and KSN = 10 bytes. For AES-DUKPT, BDK = 16, 24, 32 bytes (depend on AES key size) and KSN = 12 bytes.

The encryption is completed with a unique derived key. It is normally used to encrypt the PIN or card information of consumer obtained via means of point of sale (POS) devices. Features of DUKPT scheme are-

i) It permits sender and receiver parties to be in settlement to key used for a given transaction.

ii) It enables every transaction to have specific key from all other transactions. Each device generates an exceptional key sequence.

iii) If derived keys (in use) get compromised, past and future keys stay uncompromised.

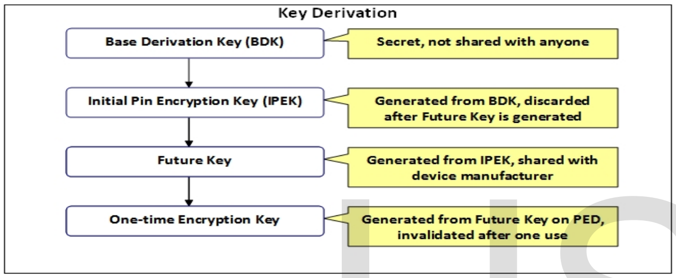
Key Derivation
Base Derivation Key (BDK)
Secret, not shared with anyone
Initial Pin Encryption Key (IPEK)
Generated from BDK, discarded after Future Key is generated
Future Key
Generated from IPEK, shared with device manufacturer
One-time Encryption Key
Generated from Future Key on PED, invalidated after one use

Fig. 1.Key Derivation [6]

The problem before DUKPT was the undesirable need for a table of encryption keys as numerous as devices deployed, as there has been Master/Session key scheme utilization which required each PIN encrypted device to be initialized with a unique master key. DUKPT resolved this as all the initialization keys of a whole family of devices are derived from a single key called as base derivation key (BDK).The algorithm needs an preliminary key which was initially referred to as super secret key, however renamed to as Base derivation key(BDK). The parties that know this key is, the party which initializes the encryption and the recipient of encrypted messages. The basic outline of the process can be explained as [2]-

i) The Base derivation key alongside device’s KSN (Key serial number) is used to generate Initial PIN encryption key for the device.

ii) This IPEK is used to irreversibly generate a list of future keys, one of the future/session key can be used to encrypt the consumer’s message or card information.

iii) After one swipe by the user, the KSN value will be incremented by one and used future key will be discarded.

Flow process of encryption of data using DUKPT key management scheme with the help of AES and 3DES [6]-

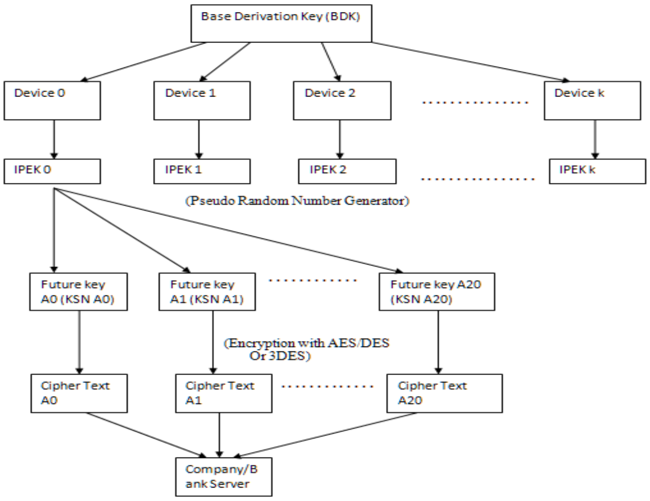

Fig. 2. Flow Process Diagram [6]

6 DES AND AES CHARACTERISTICS

6.1 Data Encryption Standard

DES is a symmetric block cipher algorithm depicted in Figure 1 it takes 64-bit block size as an input and gives 64 bit as a Cipher Text. DES uses 64bit block size and 56-bit key size, after execution of the algorithm, a 64-bit cipher is produced [18]

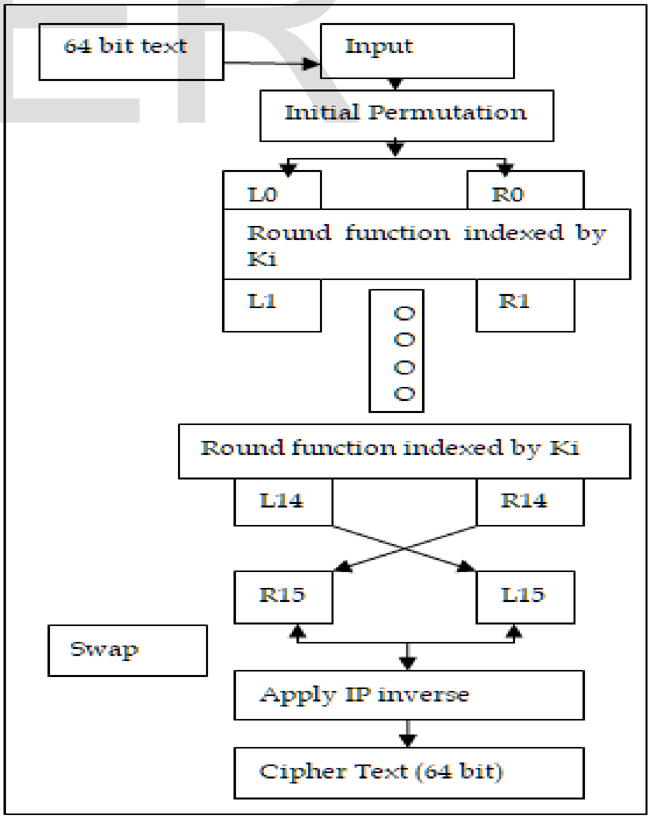

Fig.3. Flow chart of DES encryption process [18].

Key Generation: Figure 3 explains the working of round key generation. The original key of 64 bit length is given to parity drop function to get a cipher key of 56 bits, the remaining 8 bits can be used for error checking or other work. After this the 56 bits key is divided into two parts of 28 bits each and followed by 16 rounds of key generation. The rounds works in a fashion where in rounds other than 1,2,9,16 the bits are shifted by 2 bits and after shifting in each round both parts are combined and compressed using P-box to get a round key of 48 bits.
TDES is performing DES encryption or decryption 3 times using the same key generation, applying round keys 3 times for encryption the mode is (E-D-E) and for decryption the mode is (D-E-D).

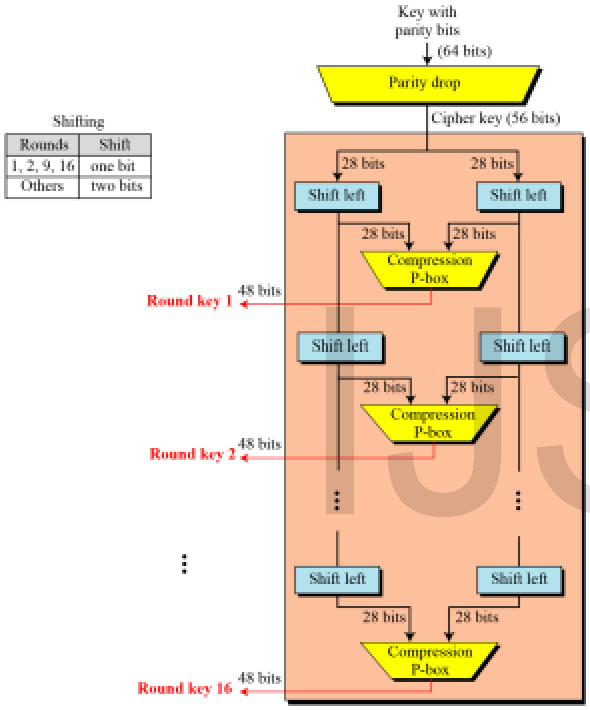

Fig. 4. Key generation [18]

DES function: Figure 4 explains the expansion and compression of the round keys, expansion is needed to match the length of key and plain text. The 32 bit plain text is expanded using the expansion P-box to get a 48 bits text which is then xored with the 48 bit round key to produce a 48 bit text which is again compressed using S-Boxes to get 32 bits text, which is then permuted using P-Box to get 32 bit output.

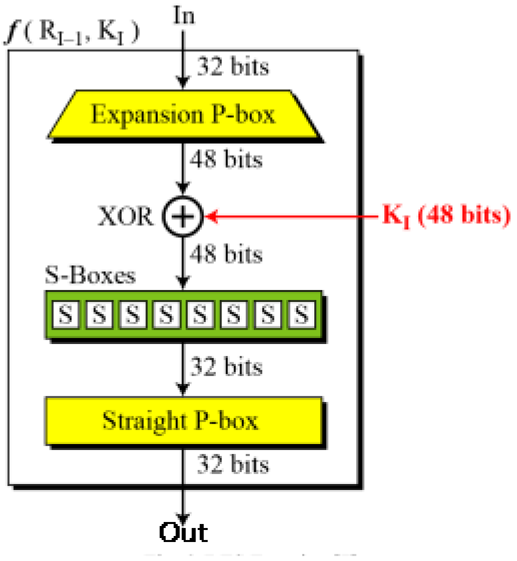

Fig. 5. DES Function [18]

6.2 Advanced Encryption Standard

This standard specifies the Rijndael algorithm [9], [20], a symmetric block cipher which can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle further block sizes and key lengths, but they are not adopted in this standard. For the AES algorithm, the length of the input block, the output block and the State is 128 bits. This is represented by Nb = 4, which reflects the number of 32-bit words (number of columns) within the State.

	Key Length *(Nk words)*	Block Size *(Nb words)*	Number of Rounds *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Fig. 6. Round number and Round key for 3 versions [20]

Figure 7 explains the working of encryption process of AES cryptographic algorithm.

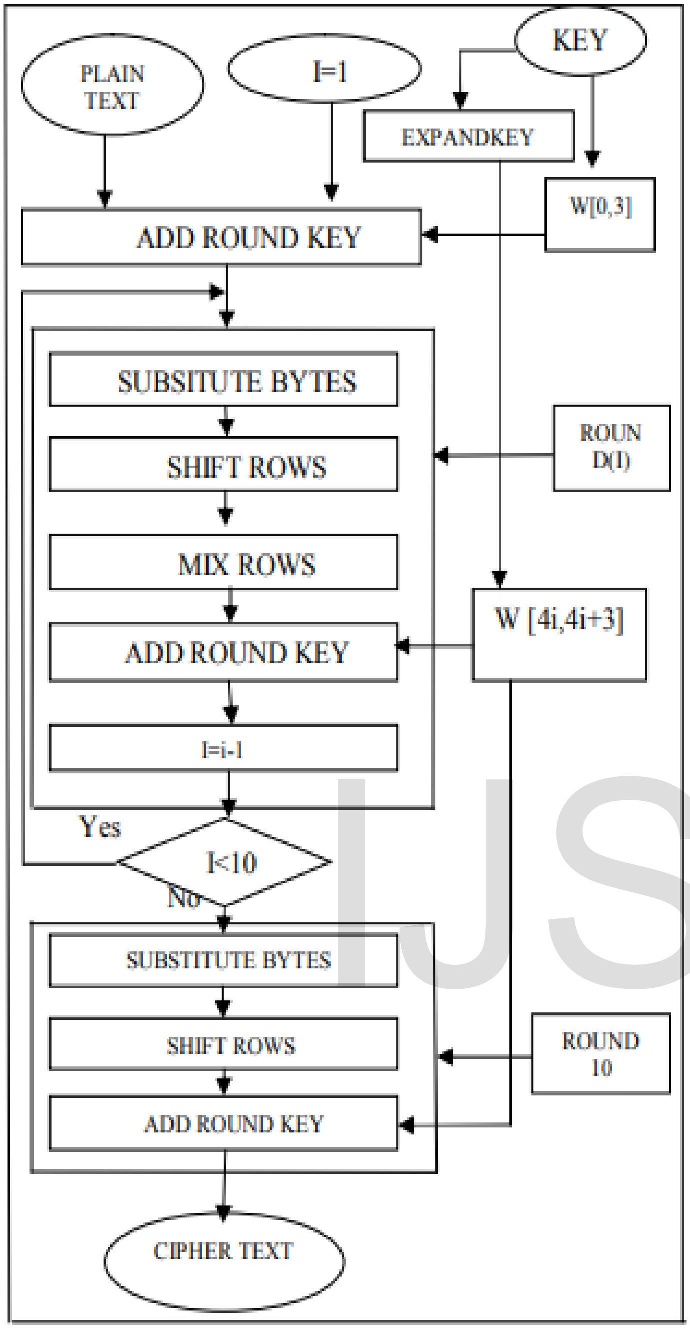

Fig. 7. AES Encryption block diagram [20]

7 Implementation and Results

Implementation of card data encryption and decryption is done on a system having windows 10 with Intel core i3 @1.50 GHz processor and 4GB ram, and performance and results are calculated using Jupyter notebook IDE, implementation is done in node JS using the dukpt package written in node JavaScript and import as package using node package manager and python programming languages.

The results are shown in tables below (code is run several times to get the average encryption and decryption times)-

TABLE 1
RESULTS OF ENCRYPTION IN HEX ENCODING SCHEME

	Using AES/3DES in Hex Encoding	
	AES(128 bit)	3DES(64 bit)
Encryption time(ms)	3.12	1.45
Decryption time(ms)	2.18	0.54
Encryption throughput(B/ms)	20.47	44.162
Decryption throughput(B/ms)	13.74	54.694

ms=milliseconds,Hex=hexadecimal,B/ms= Bytes/millseconds

TABLE 2
RESULTS OF ENCRYPTION IN ASCII ENCODING SCHEME

	Using AES/3DES in ASCII Encoding	
	AES(128 bit)	3DES(64 bit)
Encryption time(ms)	4.38	1.71
Decryption time(ms)	3.37	0.566
Encryption throughput(B/ms)	14.61	37.22
Decryption throughput(B/ms)	18.97	113.01

ms=milliseconds,Hex=hexadecimal,B/ms= Bvtes/millseconds

The heap memory used by 3DES encryption is approximately ~ (7-8.5 MB) and by AES encryption is approximately ~ (6-8 MB) in the system.

From the above results it can be seen that average encryption and decryption throughput of 3DES is more as compared to AES using DUKPT scheme in practical than in the theoretical results. As we know AES encryption algorithm provides complex results and high security to a system that is why it uses more time and less memory in this implementation than 3DES encryption algorithm is using.

8 Future Scope and Conclusion

Cryptography plays very important role within the security to take care of the confidentiality, authentication, integrity and non- repudiation of the information with the help of a highly secure key management scheme for securing user data.

Symmetric Encryption with the help key management scheme like DUKPT provides security and efficiency to the digital payment systems. The above results are useful in improving the performance of the scheme for implementing any secured payment system or application.

REFERENCES

[1] Eric Brier and Thomas Peyrin, ”A Forward-Secure Symmetric-Key Derivation Protocol How to Improve Classical DUKPT”, International Association for Cryptologic Research 2010

[2] Amal saha, Sugata sanyal, ”Applicability of DUKPT Key Management Scheme to Cloud Wallet and other Mobile Payments”**,** International Journal of Computer Applications 108(8), Dec 2014

[3] Saptarshi Mitra, Bappaditya Jana, Jayanta Poray, “Implementation of a novel security technique using triple DES in cashless transaction”

[4] Vivek Kumar Singh, Shubham,” Security in Digital Payment”, International Journal of Advance Engineering and Research Development Volume 4, Issue 11, November -2017

[5] Bawna bhat, Abdul Wahid Ali, Apurva Gupta,”DES and AES performance evaluation”, International Conference on Computing, Communication and Automation (ICCCA2015)

[6] American National Standards Institute. ANSI X9.24-1:2009 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques (2009)

[7] Zachary, O., Masese, E. and Wanyembi, G., “Security and privacy of electronic banking”, International Journal of Computer Science Issues, Vol. 9, Issue 4, 2012

[8] A. Aruna, Devansh Sharma, Manikanta Elluru, Subha Sarkar,” Securing Online Transactions with Cryptography And Secured Authentication Methods”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019

[9] “Advanced Encryption Standard (AES)” Federal Information Processing Standards Publication 197, Nov. 26, 2001

[10] Tiwari M., Kumar R., Jindal S., Sharma P., Priyanshu (2013) An Efficient and Secure Micro-payment Transaction Using Shell Cryptography. In: Singh K., Awasthi A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 115. Springer, Berlin, Heidelberg

[11] Ren F., Chen L., Zhang T. (2011) 3DES Implementation Based on FPGA. In: Zhiguo G., Luo X., Chen J., Wang F.L., Lei J. (eds) Emerging Research in Web Information Systems and Mining. WISM 2011. Communications in Computer and Information Science, vol 238. Springer, Berlin, Heidelberg

[12] Jana, Bappaditya & Poray, Jayanta. (2016). A performance analysis on elliptic curve cryptography in network security. 1-7. 10.1109/ICCECE.2016.8009587

[13] S. Kamara and K. Lauter. Cryptographic cloud storage. In Financial Cryptography and Data Security (FC’10), volume 6054 of LNCS, pages 136–149. Springer, 2010

[14] Sirbu , M. Tygar, J.D. “NetBill: An Internet commerce system optimized for network delivered services” 40th IEEE Computer Society International Conference (COMPCON'95). Mar 1995

[15] Vyas, S., Impact of E-Banking on Traditional Banking Services, International Journal of Computer Science & Communication Networks, Vol. 2, Issue 3, 2012

[16] Zachary, O., Masese, E. and Wanyembi, G., Security and privacy of electronic banking, International Journal of Computer Science Issues, Vol. 9, Issue 4, 2012

[17] Dr. Yousif AL-Bastaki Dr. Ajantha Herath.”Secure Digital Cashless Transactions with Sequence Diagrams and Spatial Circuits to Enhance the Information Assurance and Security Education”, International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012

[18] Mukta Sharma,Dr RB Garg,” DES: The Oldest Symmetric Block Key Encryption Algorithm”, 5th International Conference on System Modeling & Advancement in Research Trends, 25th_27'h November, 2016”,SMART-2016 IEEE conference

[19] Stallings, W. (20 I I). Cryptography and Network Security: Principles and Practice. US, USA: Pearson

[20] V. Rijmen and J. Daemen, “design of Rijndael; AES–TheAdvanced Encryption Standard,” Springer-Verlag 2002

[21] Harshita Prasad,Divya Sharma,Jyoti kandpal,Gaurav Verma,”Design of low power and secure implementation of S-BOX for AES”, 2016 International Conference on Computing for Sustainable Global Development (INDIACom),IEEE 2016

[22] Sai Anand R., Madhavan C. (2000) An Online, Transferable E-Cash Payment System. In: Roy B., Okamoto E. (eds) Progress in Cryptology —INDOCRYPT 2000. INDOCRYPT 2000. Lecture Notes in Computer Science, vol 1977. Springer, Berlin, Heidelberg

[23] Fiolitakis Antonios, Petrakis Nikolaos, Margaronis Panagiotis, Antonidakis Emmanouel, "Hardware Implementation of Triple-DES Encryption/ Decryption Algorithm", International Conference on Telecommunications and Multimedia, conference paper year (2006)