AES encryption and MD5 hash function along with steganography to make secure money transaction

Ekta Chauhan
Dept of computer science Engg.
Maharana Pratap College Of Technology
Gwalior, India
ektachauhan81@gmail.com

Abstract:

E-commerce is procedure of business performance by computer networks. A person using the computer can access every Internet facility to sell or buy the goods. Unlike classical commerce that is carried out physically with person effort to go & get products, e-commerce has made it simpler for human to decrease physical work and to the save time. Now a day a problem creates money transaction security. Currently cryptography permits person to the carry over confidence found in the physical world to the electronic world, thus the user authorizing to attain business electronically without worries of deception and deceit. Each day numerous user interact electronically work, whether it is by e-mail, e-commerce, ATM machines, or cellular phones. Transmitting data or document can be done through these ways will be secured. In this paper enhance data security with the help of AES algorithm and MD5 hash function along with a steganographic algorithm like LSB substitution technique and compared the performance of encrypting methods which based on the stimulated time analysis at encryption and decryption procedure time.

Keywords: AES, DES, RSA, Steganography, etc.

INTRODUCTION

Systems of e-payment is central to on-line business procedure as corporations look for ways to serve user faster and consume minor cost. E-payment systems and e-commerce is extremely linked given that an online user must pay for services and products. Obviously, the payment is the mercantile integral part procedure and prompt payment is crucial. If the debits and the claims of the several participants (banks, consumers and companies) because of payment delay there are not balanced, then the chain of the whole business is disrupted. Hence significant E-commerce aspect is prompt and secure clearing, payment, and settlement of debit or credit claims. The wholesalers also progressive commercial law nearby the same instruments use that proved to be one of the rotating points in the commerce and trade history. We are on the verge of a alike sort of improvement currently, but one that is unlikely to proceed anywhere near centuries it took for the classical payment system to evolve. Everybody decides that the settlement and payment procedure is a possible bottleneck in rapid E-commerce atmosphere if we rely on conventional payment approaches, for example, cash, cash, checks, bills or bank drafts of exchange. Such as, small denominations payments must be prepared and accepted through vendors in real time for knowledge snippets.

Conventional instruments are too much slow for micro-payments and costs of high transaction conclude in processing them add significantly to the overhead. Therefore, novel payment techniques are required to meet the emerging e-commerce demands. These nonpayment instruments must be protected, have a cost of low processing, and be accepted extensively as global currency tender. [1]

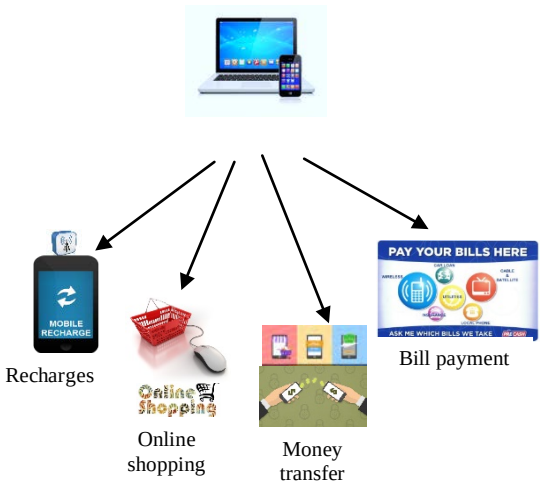


Figure 1: E-commerce money transfer by different mode of payment

ELECTRONIC TRANSACTION VS PAYMENT

We create a difference between *E-payment* protocols *and E-transaction* protocols. While E-payment deals with actual transfer of money, protocols of E-transaction deals with transactions as a whole. This concludes: service acceptance, service delivery, receipts, payment confirmation, etc. Both are the most significance for E-commerce systems. E-transaction protocols set together operations and the failure of implement atomicity, serializability and permanence. An E-transaction either fails or each of its operations are carried out (*failure atomicity*). If money transaction fails all in part completed outcomes will be undone. Every transaction that whole effectively cannot be undone, and the transaction outcomes are not lost (*permanence*). The transaction results that are carried out concurrently will be the similar as if they were carried out serially (*serializability*).

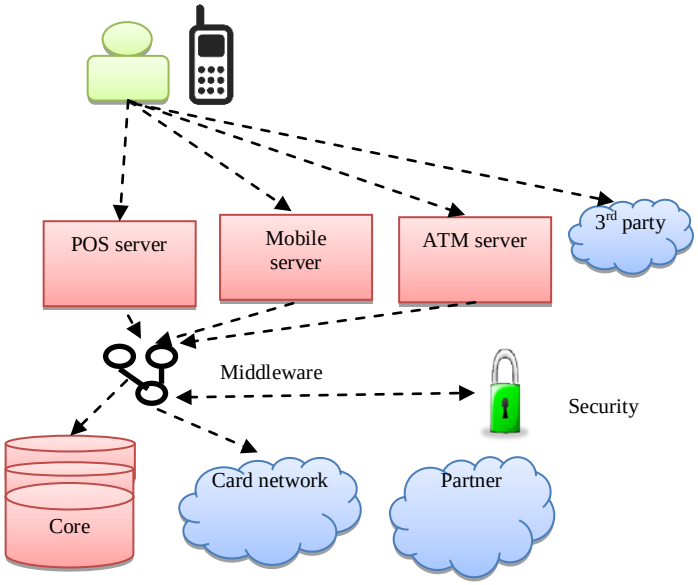


Figure 2: Basic money transfer

Protocols of E-payment transfer trust, either as digital cash, or as cryptographically signed promises. Signed promises prove the sender authenticity and sender's intention to pay for a facility. This is, basically, how systems of credit card work. Digital cash is signed data representing real currencies. These data do not carry any sender identification and are by themselves anonymous. E-transactions and E-payments are orthogonal problems and solve various issues. A key point is that payment itself is commonly only a small interaction part with a service provider, and a system that implements E-commerce must also implement various ingredients of E-transactions. For example, if a merchant service performs with digital cash, but cannot prove afterwards that service was essentially paid for, the system will not be much secure for individuals. [2]

MODE OF E PAYMENT

The E-payment system is an online business procedure used for fund transfer applying electronic means like personal computer, mobile phones, etc. They are widely used in bank whenever transactions are made in terms of payment and other means. The various modes of E-payment are Smart Cards based E-Payment System, Debit Card Payment System, Credit Card Payment System, Online E-Cash System and E-Cheque System. Each payment system has its benefits and drawbacks for the merchants and customers.

The most functional e-payment sources are as follows:

- Debit Card
- Credit Card
- E-Cheque
- Electronic Fund Transfer (EFT)
- Smart Card
- Electronic Transfers

There are various approaches for e payment have basic need, e.g. anonymity, traceability, acceptability, security, convenience, cost and control. Therefore, focusing instead on the

technological of various systems of E-payment specifications, the researcher has distinguished systems of E-payment based on what is being transmitted over network [3].

IMPORTANT SECURITY REQUIREMENTS

The basic aim of cryptography is to secure significant knowledge as it passes from a medium that may not be protected itself. There are various cryptographic algorithms, all of which can provide one or additional of the following facilities to applications. It is commonly accepted that, in order to be considered secure, system of payment must fulfill the following fundamental security need.

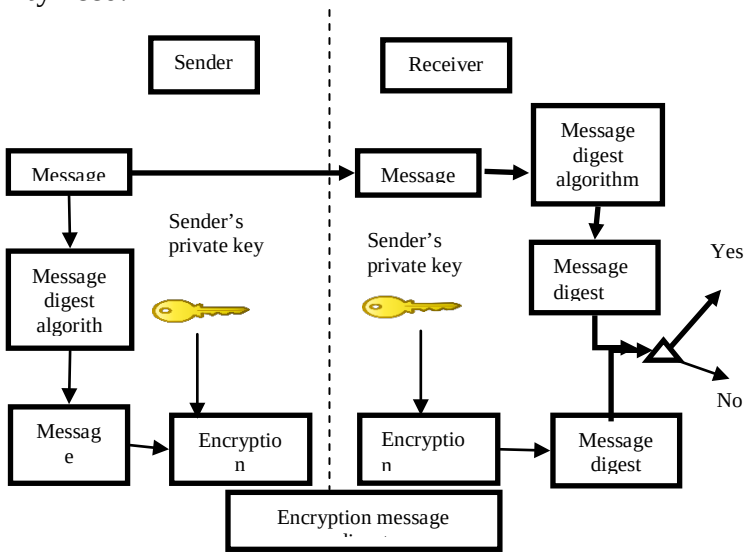


Figure 3: Secure Electronic payment

Authentication

Communicating parity assurance is one that is claimed to be masquerade parties prevents conclude in the money transaction. Both parties should be able to comfortably with working the money transaction that they are communicating with the party with whom they think they are communicating. Applications generally achieve authentication checks by security tokens or through verifying digital certificates issued with the help of certificate authorities. Cryptography can use to create any user identity for secure authentication purposes.

Access Control

The unauthorized use, prevention of a resource (i.e., this facility controls who can contain access to a resource, under what situations access can happen, and what those accessing the resource are permitted to do.)

Data Confidentiality (Secrecy)

The data protection from unauthorized disclosure. Confidentiality is an important component in customer privacy, as well as in the proprietary knowledge Protection, and as a deterrent to theft of knowledge facility. The only way to confirm confidentiality on a public network is by strong encryption. The information is kept secret from those without the complete credentials,even if that information travels from an insecure medium

Data Integrity (Anti -tampering)

The assurance that information received are exactly as sent through an authorized entity. Prevents the information unauthorized medication. Financial data travel by multiple routers on open network to reach their destinations. Here must make sure that the data is not changed in transit.

Non-Repudiation

Provides protection against denial through one of the entities involved in a communication by containing participated in part of the communication. Non-repudiation, Origin- Proof that the data was sent through an identified party.

Non-repudiation, Destination- Proof that an identified party send information. Non-repudiation is usually provided through digital signatures and public key certificates [4] [5] [6] [7].

TYPES OF E FRAUDS

In order to assess the risks of and combat payment fraud, there should be an understanding of its many facets. E-payment frauds have a multiplicity of types and there is no exact number or fixed list of these types. Frauds are classified as online fraud and offline frauds. Online frauds occur when a fraudster possesses legitimate company to find sensitive personal data and unlawfully conduct money transactions in the present accounts. Online frauds occur when a fraudster steals user secret data, for example number of credit, number of bank account or other different identification and uses it constantly to open a new account or pledges transaction in the real individual/company‟s name. Department of Justice (DOJ) U.S has divided frauds(computer fraud) into three categories: 1) crimes in which system hardware, peripherals, and software are the main aim of a crime; where in the fraudster gets objects illegally: 2) crimes in which the computer is the immediate crime subject, that is the attacks is on a system or a computer, disrupting or destruction of which is the injury caused. There are different types of e-fraud and all of these attacks in a slightly different way. Fraud can occur in a number of ways as listed below.

Account Hacking: Hacking includes gaining illegal entry into a person's computer (PC) system. Fraudsters use compromised customer credentials to origination system hijack and use it in lawful account holder‟s name. Corporation are also targeted and also seen on a rise. Attacks are aimed

Identity theft: Identity theft/fraud refers to crime in which fraudster illegally finds and uses other user personal information in some way that conclude deception. Identity theft/fraud is the most serious crime for the person whose information is stolen as well as the financial institution.

Phishing: Phishing is a well-known technique for obtaining confidential information from a user by posing as a trusted authoring. Phishing is an attempt by fraudster to „fish‟ for your details of banking by emails with attachment or hyperlinks. The e-mail appears to be sent from legitimate organization to trick people in order to reveal sensitive information. On clicking the attachment or the hyperlink the computer system gets infected with malware. Malware or „Malicious Software‟ is software which includes computer viruses, worms, spyware, Trojan Horses and other various malicious software.

Spoofing or Website cloning: This is an act of creating a hoax web site or to say duplication on a website for criminal use. This usually takes the form of know chat room or trade sites

where people would innocently give out personal information to criminals or make a fake purchase of a product the does not exist.

Internet Gambling (Virtual casinos): The Internet has made certain types of gambling possible. A person in India or china from his home can participate in an internet poker game in the Caribbean over the Internet. CERT-LEXSI (2006) as cited by McAfee (2009) there are around 15000 active online gambling sites in 2006 out of which 1766 operate on license. Online gambling establishment disappear and appear with regularity, collecting from losers and not paying winners without any fear of being appended and prosecuted.

ACH Frauds: ACH Fraud is essentially a data fraud. With the growth in ACH transactions for corporate payments obviously there is an ACH frauds increase. The fraudsters access the account information and route number illegitimately to steal funds directly from accounts. Government payment, payroll and other online payment face these frauds.

Check frauds: Check frauds continue to be a threat to financial security. E-check frauds can be easily committed; the fraudster needs scanner, printer and desktop phishing software. The most common forms of check fraud include altering check, forging endorsement, counterfeiting checks and creating remote checks. According to the AFP Report (2011) 14% of the victims of the organization suffered financial loss due to check fraud.

Lottery frauds: One will receive scam emails informing of winning a substantial money amount in a lottery draw. When the receiver reply‟s, the sender then asks for bank account details and various personal data so they can transfer the money. These emails are fake and may ask to pay a handling feel that will lead to loss of money and your personal data which may be used in other fraud.

“Nigerian advance fee fraud (419 fraud)” This e-fraud is the most popular and lucrative fraud, which is named after the section of Nigerian law that covers it “419”. The hoax often arrives with a bulk mailing or family member email of asking the recipients to enter into business and getting money transferred with huge commission in return. Once the contact is established the fraudsters request money in advance which need opening of an account in the bank or paying some fee which leads to trouble and expenses. [8]

ADVANCE ENCRYPTION STANDARD

AES is based on Rijndael cipher, symmetric 128-bit block information encryption method that has been established through Belgian cryptographers J. Daemen and V. Rijmen [9]. AES symmetric block cipher ratified as a standard by NIST. This has been select applying a procedure lasting from 1997 to the 2000 that was decidedly more transparent and open than its predecessor, the aging DES [9]. AES is based on the design principle called a substitution-permutation network, permutation and substitution combination, and is software and hardware fast. AES is applying for many key lengths: 128, 192, or 256 bits. Encryption contains of 14 rounds for 256-bit keys, 10 processing 128-bit keys and rounds, 12 rounds of 192-bit keys. Each round is identical for the keys except the last round.

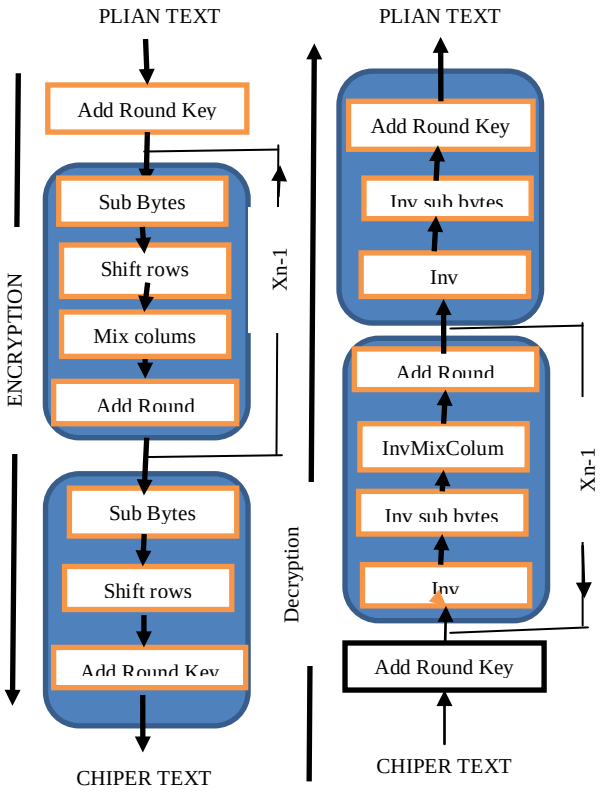


Figure 4: Advance encryption standard

MD5 message diagest

In 1999 Ron Rivest designed an MD5 message-digest algorithm to swap a previous hash function, MD4. MD5 algorithm is commonly used cryptographic hash function, making a 128-bit hash value, typically expressed in a text as a 32 digit hexadecimal number format. MD5 has been in an extensive cryptographic applications variety, and is also usually used to confirm information integrity [10]. The basic concept behind this algorithm is to assume a random information (binary or text) as an input and make a fixed size “hash value” as the output. The input data can be of any length or size, but output “hash value” size is each time fixed. Here is an example of MD5 Hash function at work:

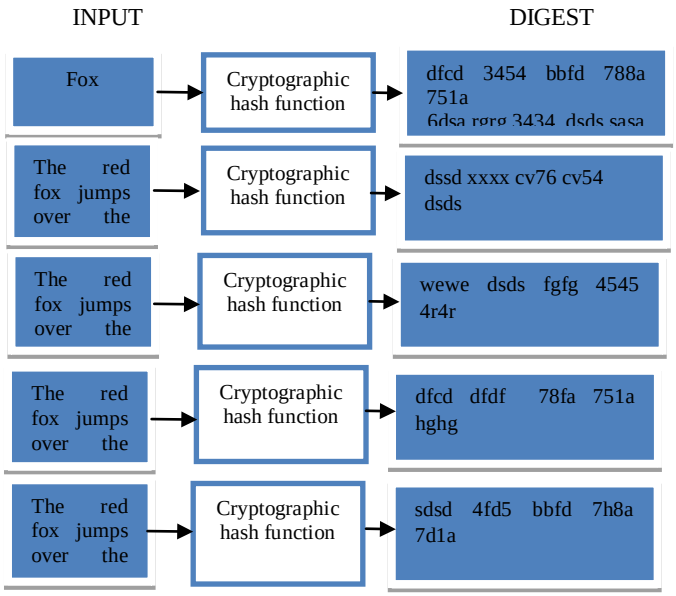


Figure 5: MD5

STEGANOGRAPHY

Steganography is the art or practice of hiding a file, information, video or image within another video, file, message, or image. Steganography advantage over cryptography is that intended secret information does not attract attention to itself as a security object. Thus, whereas cryptography is protecting practice information contain, steganography is concerned with concealing factual that a secret data is being sent, as well as concealing data contents. The primary steganography objective is to avoid drawing attention to the hidden knowledge transmission. If suspicion is raised, then this objective that has planned to attain data security because if the hackers noted any modification in the sent data then this observer will try to know hidden data inside the other data [11] [12].

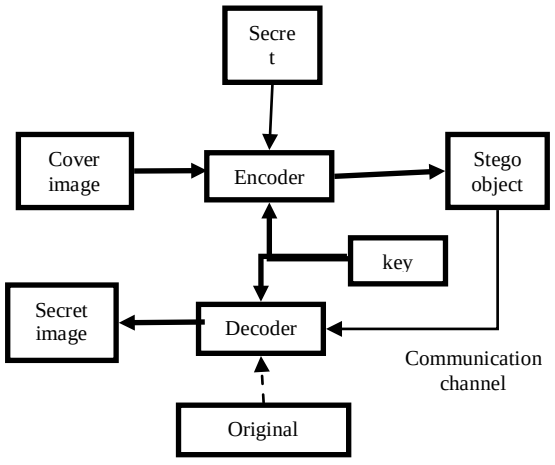


Figure 6: Block diagram of steganography

LITERATURE SURVEY

Md. Khalid Imam Rahmani (2014) et al present that The two valuable security aspects that deal with transmitting knowledge or information over few medium for example Internet are cryptography and steganography. Both of them are used to confirm security. But none of them can easily achieve the simple security need i.e. the features for example robustness, capacity and undetectability etc. So a novel technique based on combination of both steganography and cryptography known as Crypto-Steganography which overcome all other's weaknesses and create difficult for the intruders. This paper also defines the basics cryptography and steganography concepts on the basis of previous literatures presented on the topic. [13]

B. Padmavathi (2013) et al present sharing the data over the internet is becoming a serious problem because of security issue. Hence, more methods are required to protect the shared information in an unsafe channel. The current work focus on a combination of steganography and cryptography to secure the information while transmitting on the network. Encrypted information must be hidden in an image or audio or video file with using steganographic algorithm. Last with the help of applying the decryption method the receiver can view the original information from the hidden image or audio or video file. Transmitting information or data can be complete by these ways will be secured. In this paper implemented three encrypt methods, for example DES, AES and RSA algorithm along with steganographic algorithm, for example, LSB substitution method and compared their encrypt technique analysis based performance of its stimulated time at the decryption and encryption procedure time and also its buffer size experimentally. [14]

Shristi Mishra (2015) et al present that Cryptography and Steganography are two popular methods that are more widely used for sending information in a secret way. The cryptography and steganography purpose are same. Both are used to protect important data, but in various ways. Cryptography scrambles knowledge so that it can't understood and steganography data hides so that it cannot be seen. Cryptography is not capable of hiding the presence of data alone and it cannot protect data effectively. An eavesdropper can easily detect encrypted information presence. This paper focuses on merging steganography and cryptography approaches strength. This paper also defines cryptography and steganography main concept. [15]

Hemang A. Prajapati (2015) et al present that In last few years communication technology has been enhanced, which increase the secure data communication need. There is a technique used for significant information imperceptibly hiding, which is Steganography. Steganography is the hiding knowledge art in such a way that prevents hidden data detection. Applying steganography procedure in conjunction with cryptography, known as Dual Steganography. This paper tries to elucidate the common steganography concepts, its several methods and kinds, and dual steganography. There are also few of research works achived in the steganography field in the previous few years. [16]

Moses Okechukwu Onyesolu (2012) et al present that The advance in e-transactions have resulted in a better demand for accurate and fast user authentication and identification. A conventional identification technique based on the ID possession cards or exclusive information like a password or a social security number are not each together reliable. [17]

PROPOSED METHODOLOGY

In secure authentication and e- payment system must be sure to secure our information like our password which may be biometric identification such as fingerprint, iris, voice, etc. in this paper, we focus on AES encryption with MD5 algorithm and Stenography with applying pixel swapping to encrypt the input image for the secure transaction purpose. This paper has a target on compress the time of encryption and decryption adopting multithreading. Consider following conspiracy to explain the proposed work.

At sender side-

1. To convert the first picture into binary code.
2. Divide binary code into obstructs, all pieces contains 16 characters (128bits).
3. Apply AES encryption procedure to change over plain text hinders into cipher text block.
4. AES Algorithm has the accompanying steps.

The main step is taking info plain content, then apply Key Expansion-Round keys are derivational from the figure key applying Rijndael's key calendar. Starting Round (Add Round Key- singular byte of the state is joined with the round key utilizing bitwise XOR) Rounds (Sub Byte singular byte is supplanted with another from lookup table. Movement Rows individual line of the state is cycle moving. Blending Columns- a blending procedure which works on the segments of the state, consolidate the 4 bytes. Include Round Key) Final Round (Sub Bytes, Shift Rows, then Add Round Key)

5. Transfer these cipher text into binary code.
6. Encrypt picture is inserted into the cover picture by utilizing an LSB method by applying stego key and discovering a picture is called stego picture and apply the Algorithm of Pixel Swap utilizing a pseudo–random succession than send to the recipient.
7. After hash code embedding of the cover image samples is produced applying MD5 hash algorithm.
8. The hash code is embedded inside cover audio and stego image is produced.

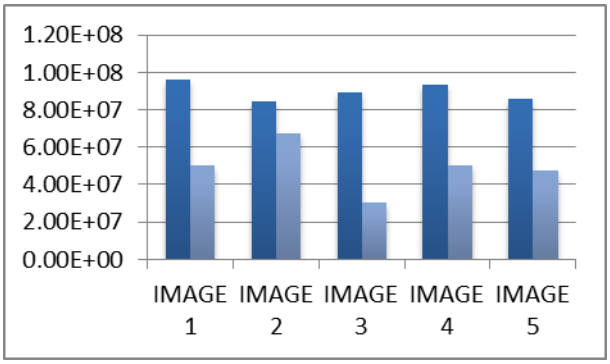
At receiver side-

1. Change the got picture into binary code.
2. The receiver then extracts hash code embedded inside stego image.
3. The hash stego code samples are produced and compared with extracted hash code.
4. The image sample's integrity is verified, if both codes match. Otherwise the data are intercepted or corrupted.
5. Embedded stego binary picture into figure content bit and translating, select the pixels utilizing the same Pseudo-irregular arrangement.
6. Convert the content and isolated into pieces, every one of the 16 characters.
7. Application unscrambling procedure to a cipher code piece of discovering a secret picture purpose.

Result simulation

Figure 6: Figure print image

Figure 7: Covered image



Graph 1: Total time difference in base and proposed work

Conclusion

Secure electronic payment system for Internet transaction. The system of security architecture is designed through applying Numerous Security techniques and Protocols, which removes the fraud that happens today with stolen credit card/debit card payment knowledge and customer data. E-commerce include the exchange of some money form of services and goods over the Internet, but today, the Internet is an unconfident and untrustworthy media. In E-commerce area security and privacy are still ongoing research issue. There have been few significant and interesting findings, however, in the previous few years that bear significant consequences for E-commerce consumers and sites. Privacy is now understood, though numerous, to be a social construction with expectations the main consideration. Privacy is a considered a public issue with regulators, who have nonetheless mainly permitted technology to unfold to date. Security is now understood to be mainly imperfect, a continual game of hacking and security expert. Developments of Important technical have been deployed in the previous few years; however, it is clear that organizational policies may perform as significant a role in site security. In this paper, we define a new technique to secure user information, using AES encryption and MD5 hash function along with a steganographic algorithm like LSB substitution method and compared their encrypt method performance based on the stimulated time analysis at encryption and decryption procedure time.

References

[1]. Ms.Vaishnavi.J.Deshmukh, Sapna.S.Kaushik and Mr. Amit.M.Tayade,” Payment Processing Systems and Security for E-Commerce: A Literature Review”, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-5), May 2013,pp:29-35.

[2]. Paul J.M. Havinga, Gerard J.M. Smit, Arne Helme,” SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS”,

[3]. Manav Aggarwal,” E-Payment”, Volume : 3 | Issue : 10 | Oct 2014, PARIPEX - INDIAN JOURNAL OF RESEARCH,pp:33-34.

[4]. ELECTRONIC CASH AND SET, Paper presented at the conference: Internet Crime held in Melbourne, 16-17 February 1998.

[5]. Gary C.Kessler, N.Todd Pritsky,”Internet Pay ment Systems: Status and Update on SSL/TLS, SET and IOT P” Info rmation Security Magazine August 2000.

[6]. Ba ja and Nag, " E-Co mmerce" TMH Publicat ions.
[7]. Kaliski Jr, B.S. and Yin, Y. L., September 1998. "On the security of the RC5 Encryption Algorith m", 2006.
[8]. LINA FERNANDES," FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES", Asia Pacific Journal of Marketing & Management 2319-2836 Vol.2 (3), March (2013) Online available at indianresearchjournals.com
[9]. FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.
[10]. Mark ciampa, "CompTIA Security+ 2008 in Depth" Cengage Learning, 2009, ISBN 1598639137, 9781598639131
[11]. H. Wu, H. Wang, C. Tsai and C. Wang, Reversible "image steganographic scheme via predictive coding". 1 (2010), ISSN: 01419382, 35-43.
[12]. J, Corporation, Steganography. http://www.webopedia.com/ TERM/S/steganography.html. 2005.
[13]. Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal," A Crypto-Steganography: A Survey", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014, pp:149-155.
[14]. B. Padmavathi and S. Ranjitha Kumari," A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 4, April 2013,pp:170-174.
[15]. Shristi Mishra and Ms.Prateeksha pandey," A Survey on Crypto-Steganography", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 2 081– 084, February 2015
[16]. Hemang A. Prajapati and Dr. Nehal G. Chitaliya," Secured and Robust Dual Image Steganography: A Survey", International Joural of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015,pp:30-37.
[17]. Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani," ATM Security Using Fingerprint Biometric Identifer: An Investigative Study", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012,pp:68-72.