Roll. No. A016	Name: Varun Khadayate
Class B. Tech CsBs	Batch: 1
Date of Experiment: 10-09-2022	Subject: Cryptology

Aim

Study of cryptology in e-commerce applications

Abstract

Internet business/ Electronic Business is viewed a a decent option with lower exchange fee and more business w y to deal with all clients across the globe. We speak to numerous unbalanced methodologies which are utilized in Web based business to closed electronic exchange and different cryptographic calculations that are primary fascination in setting up of Internet business. Electronic business is needy u on a collection of perils, for instance, unapproved access, misappropriation, change, and devastation of both data and structures.

Introduction

Advancement of Internet business can be credited to a technological development and online business is a large business and expanding dramatically. It conducts transactions through web additionally called as open public network i.e., mostly viable to execute an assortment of online business operation. A wide diversity of trade is directed through internet business, including cash move, store network, web marketing, EDI, and so on. Internet business is currently being utilized in a wide variety of business including administration firms, retail locations, and so on where Internet business has created all cycles more dependable.

Today, Security and protection are a significant worry for online business. In Web based business, numerous security problems are expanding step by step on the open web like unapproved access, customer data leakage, card clowning, and so forth. The future is probably going to be additionally disturbing as in violations will be committed without the knowledge of the victim. Preventing digital scam, later on will require a solid e-security as opposed to plain human reasonability. To build up the web-based business, security, and privacy are the fundamental driver on the Web. So, to beat the security issue, we ought to have some ensured conditions that ought to give the satisfactory assurance to the exchange data for the entire element in online business exchange.

PROBLEMS/ OBJECTIVES

Nowadays we frequently get to hear about hacking, where programmers are often discovered to take information from large-scale organizations, banks, and retailers, which present a potential danger to those information databases bases where the information makes it not reliable. To overcome this unauthenticated and criminal behavior, encryption strategies are indispensable. It requires an exceptionally critical exertion and extravagant innovation to decode this taken information with an end goal to keep your data secure.

During our existence when the Web gives fundamental consistency between the billions of individual and is used as an instrument to trade, community connection, and the trading of an expanding measure of individual data, security has significantly become a colossally issue for each client to operate on its own. This. Paper explains the significant security problem in an online business. Through the examination, the customers and the businesses to join people in a single aspect with regards to e-commerce security. By such examination of data, it generates a “Comprehensive” view. It will diminish the gap between the organization and the customer’s targets and their

understanding. By the Comprehensive view of analysis, information about a particular customer and the open web organization implements such arrangements which are adjusted to the customer needs more effectively.

LITERATURE SURVEY

SECURITY ISSUES IN E-COMMERCE:

Exchange level:

This level spotl i g h t s on transaction users that are legitimate. These r risks are emerging from the accompanying three components answer attacks, mutual validation, and no record of exchange.

- Reply Assaults: It is organizations assaults in which aggressors need. It tr ick the cryptographic convention by the re-use transmission of message over and over. The information will be legitimate and maliciously continued by the assailant advantage. This assault is done either by the source or by the foe who needs It capture the data and retransmits it. Meeting token is the strategy to Ideal with this kind of assault.
- Mutual Validation: It is likewise called two ways confirmations. On the off chance that any intruder (unapproved client) interferes with the imparting party (approved client) and commonly confirmed by them, at that point this makes the issue it approved clients.

Business integration Level:

Internet business transaction is equivalent to a transaction with non–rejection. Numerous clients may maliciously deny to the message that they send himself to recoil their duties.

- Personality Uncertain: There is a need of a virtual organization stage It the Web based-business-transaction measure where there is no need of gathering both sides. This becomes a genuine issue in Web based-business transaction because an aggressor can take the character of approved client and afterward to the exchange to get the advantage.
- Deny Transaction: Internet business transactions are same as an exchange with non–rejection issues. Numerous
  clients may deny for any message that is sent or get by them.
- Revise Transaction: Internet business shares the comparable idea of conventional business in which the exchange time cannot be adjusted.

Security Approaches in E-commerce:

Application Framework Level:

- Confidentiality It tells that only approved clients can access the data in the framework.
- Integrity: It Tells that lone approved clients can adjust any data over the organization.
- Anonymity: Just For few Webs based Business applications, it is basic to create strategies which give collectoranonymity Administrations, sender anonymity administrations, and exchange anonymity administrations.
- Non-repudiation: This guarantees that the sender cannot deny after the sending or accepting

Security Protocol Level:

Secure Socket Layer: It is a protocol layer which happens to be between the connection-oriented layer (TCP/ IP) and application layer (HTTP). TCP provide the end-to-end good service which is used by the SSL. TCP established a closed communication between client and the server by allowing common authentication.

To provide such closed services between client and the server it makes use of encryption for privacy and digital signature for integrity. It consists of four sub protocols:

- SSL handshake
- SSL change cipher spec protocol
- SSL alert protocol

- SSL record layer
- Secure Electronic Transaction (SET): Secure Electronic Transaction is correspondence convention standard and an encryption and security determination convention for making sure the credit card exchange in an open network called Internet during E-commerce exchanges. SET is not a payment framework however it is a security standard and a mix of security conventions and organizations. This empowers the clients to an online exchange through their card in an open network.

Security Validation Level:

- Message Overview: Message digest is a hashing capacity of the multitude of pieces of the message in which the correlation of the sender's and beneficiary message digest occur to identify the mistake when message pass from the open organization. Any adjustment in any piece or pieces in the message changes the consequence of the hash code. A variable size message M as a contribution to the hash capacity and it acknowledges and gives a fixed size yield message summary or hash code.
- Digital Signature e: To eliminate the issue of public key encryption (public key is known to all individual openly
  key encryption in correspondence organizations, so anybody can communicate a fashion message to the recipient and by the utilization of collector public key), we utilize advanced mark for validation. Prior to sending information content as a message, sender scrambles message content with her own private key (computerized signature), which verifies the sender in light of the fact that in organization nobody has anybody's private key.

Encryption Innovation Level:

- This innovation encodes the plain content into unreadable structure which assists with shielding the information from being seen, and it likewise gives a method to recognize if the getting information is adjusted. Encryption innovation gives secure correspondence over unstable organizations. We characterize encryption strategies in two diverse ways, as indicated by the used key.
- Symmetric Key Encryption (SKE): This is additionally called the private key cryptography or private key encryption. In this, we utilize the same key for message encryption and decoding. This key (k) is additionally called mystery key. This encryption innovation has two issues initially is Basic symmetric encryption utilized so not gives better information security and second is Issues to trade discharge-key.
- Hilter kilter Key () Encryption (HKE): It is additionally called public key encryption. In unbalanced key cryptography, we utilize two keys, one for encryption technique and other key for unscrambling strategy. One key is Public and second one is private. The public key is known to all correspondence party in organization and the private key is mystery. Each member has their own pair key (one for encryption and second for unscrambling)

METHODOLOGY

PROPOSED MODEL

E-commerce Exchanges and Volumes: To plan an Internet business set up with useful security steps, we need to characterize the online business exchanges. By definitions, we can without much of a stretch to measure the volume and development of Web based business exchanges. There are a few stages, which are trailed by the Internet business framework to use for online trade of an asset and the products and ventures first. In Online business there are a few stages

a) Gathering data: e.g., products, administrations, and value data from various sources.
b) Product debate: a detailed conversation happens about item features, value, arrangement, and numerous others.
c) Arrangement: online obligation to buy an item or administration through e-commerce

shopping and the orderto and duty to move cash in return.

d) Installment data: purchasers give installment data to the vendor.

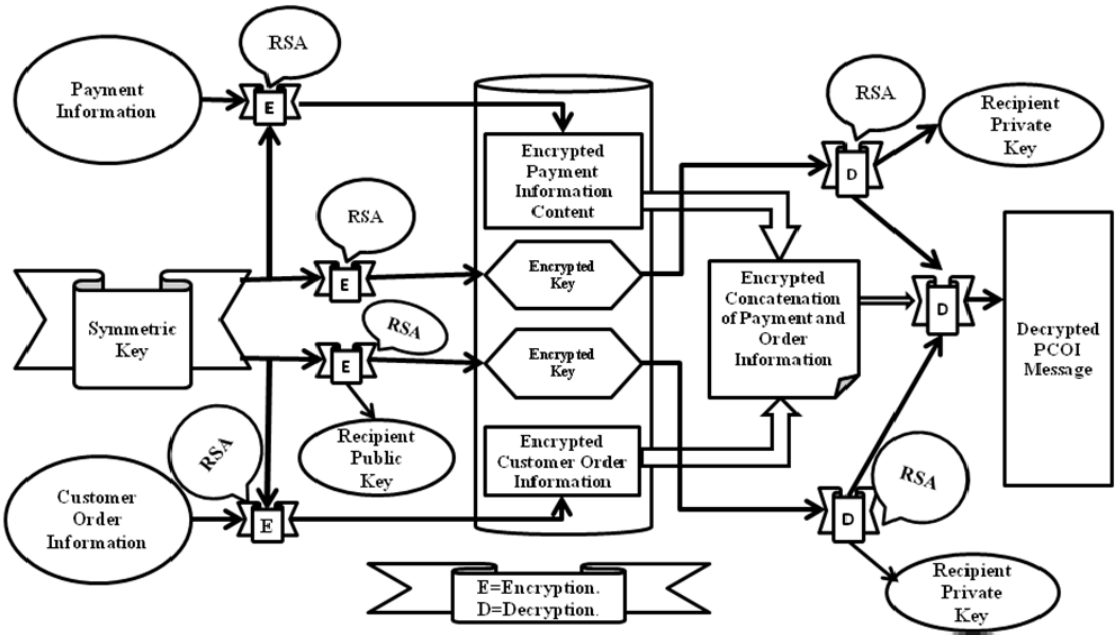
e) Delivery: vendor gives the merchandise and ventures the purchaser, and they get them.

WORKING OF PROPOSED MODEL:

We planned a model to join the installment request and the client request data under the protected calculations like IRSA. You realize that SET is secure for exchange reason in the Internet business however it is not fruitful in the e-commerce business climate since it has a ton of disadvantages.

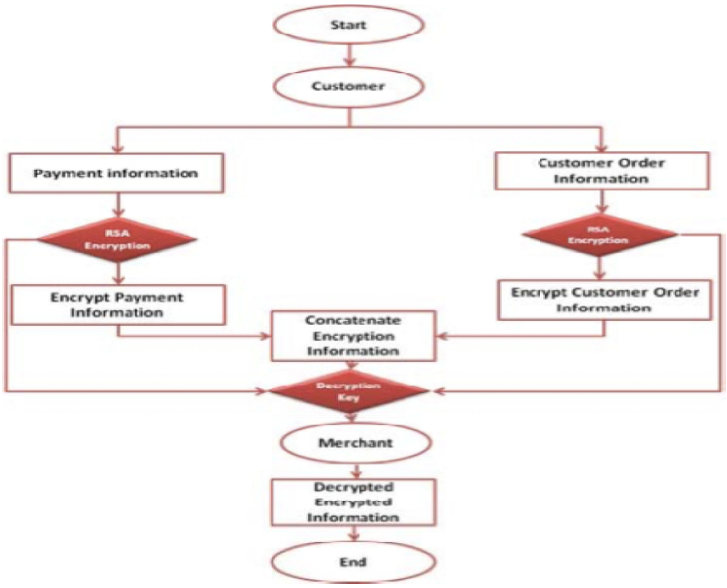
1) SET overhead is exceptionally substantial for Web based business straightforward buy exchange:
   a. Four messages are traded between the vendor and the client
   b. Two messages are traded between the vendor and the installment door
   c. Six computerized mark is registered
   d. There are 9 RSA encryption cycles and 9 RSA decoding cycles.
   e. There are 4 DES encryption/ decoding cycles.
   f. Four authentication check.
2) It has been contended by the dealers that they need to grow part of cash to handle the SET exchange from thecustomer's perspective, and furthermore need to introduce the proper programming.
3) Between operability issues are not settled.
4) Utilizing SET, installment data is secure however product's organization data is not secure.

Because of this, we proposed a model for secure e-commerce business exchanges. In the proposed model, we diminished the 4 DES encryption/ decoding cycles and the outsider CA obstruction likewise decreased from the Web based business purchase exchange. Presently, our model depends on the PGP and double mark strategy. We consolidated the two techniques which give the best outcome.



Flow Chart of the Model:

It portrays that how the client sends the goods request and installment request to the shipper to purchase the items online through Internet business arrangement



COMPARATIVE ANALYSIS

We have analyzed significant calculations identified with symmetrical cryptography. We have designated comparison table with following attributes in table 1:

1) Calculations Name
2) Features
- Computational issue.
- Encryption key size.
- Applications

3) Drawback and Attack

Initially, client will fill the online structure on web-based interface and select the item by the item id. Presently, client sends the client data request to the trader from web-based shopping online interface through Web. The other part is installment request which is necessary to purchase any item on the web.

S.No	Algorithm	Features	Drawback and Attacks
1	RSA	1) Computational problem- integer factorization problem. 2) Encryption key size-1024 bit. 3) Application- Used in all worlds banking circle for security purpose and the transaction.	1) Drawback- Key size is large, so it is 15 times slower than ECC/ Need more memory and computing power and more battery in RSA use. 2) Attacks- Chosen-cipher text attack, Discrete- Logarithm-Attack, Men-In-The-Middle-Attack.
2	Diffie Hellman	1)Computational problem- Discrete Logarithm Problem, Decision Problem 2) Encryption key size-1024 bits. 3)Application- Key Exchange	1)Drawback- The value of private key K is smaller in size which can be easily understood and decoded. 2) Attacks- It used only in key exchange only
3	DSA	1)Computational problem- Discrete Logarithm Problem 2)Encryption key size- No Encryption key in DSA 3)Application- DSA is used for digital signature.	1)Drawback- a) Vulnerable DSS design. b) The second complaint regards the size of prime 512 bits. 2) Attacks-In known message attack, attacker given valid signatures for many types of messages which is known by attacker but not chosen by attacker. In an adaptive chosen message attack, the attacker first understands and learns signatures on arbitrary messages of the attacker's needs.
4	NTRU Encrypt	1)Computational problem- Closest vector problem in lattices 2) Encryption key size- The table shows the required sizes of NTRU key strength. NTRU 251, NTRU 347 and NTRU 503 provide roughly equivalent security to RSA 1024, 2048 and 4096. Key Strength Pre-master Secret Size NTRU 25 120 bytes, 347 32 bytes and 503 48 Bytes3) Application- Digital signature	1) Drawback-"Shor's algorithm" is quantum algorithm used to integer factorization and would be able to break ECC or RSA of any practical size in negligible time period. So NTRU's security is slightly vulnerable through quantum computers. 2) Attacks- Security issues-Elementary (why N should be prime), Standard(men-in-middle attack), Implementation(choosing-cipher attack, hashing and padding issues)
5	ElGamal	1)Computational problem- Discrete logarithm problem 2)Encryption key size-512 bits. 3) Application- It used in PGP Key exchange, Authentication, encryption and decryption of small messages.	1) Drawback-The encrypted message becomes very big in size, it becomes the twice the size of original message m.ElGamal's need large amount of space to store the three part public key and two part encrypted message. 2) Attacks- Low-Modulus attack, Known-plaintext attack
6	Rabin cryptosystem	1)Computational problem- The complexity of System is same level as factoring large number n into 2 primes 2) Encryption key size-1024 bit. 3) Application- The Rabin cryptosystem can also be used to create a signature through exploiting inverse mapping.	1) Drawback-The problem is its decrypt into four possible messages. 2) Attacks- CCA attack. Algebraic attack The Hastad Attack. Algebraic Attack. Desmedt Odlyzko Attack. Related Message attack.
7	ECC	1)Computational problem- Discrete logarithmic problem 2) Encryption key size-160 bits 3) Application- Digital signature, key exchange, Authentication.	1) Drawback- It increase the size of encrypted message/It is more complex than RSA 2) Attacks- General-DL attack by SPH, Software attack estimator, Explicit attack(Hardware attack estimate, Anomalous attack,

CONCLUSION

The objective of this paper needs to expand the online business security through PGP with dual signature. Our proposed model concerns on some point like the SET security and its expense and the time utilization. In our model, a portion of the calculations are eliminated like DES. It creates numerous cycles and sets aside an excessive amount of effort to manage the information in the check however we utilized RSA calculation which is secure and less tedious. It will control all the encryption and the unscrambling with the assistance of private and public key of the sender and the collector. In this paper, we likewise examined some significant calculations which are utilized in Web banking, ATM machine, biometric framework, advanced signature, key trade, and so on.

REFERENCES

1. Ya Xin, Xua Ming ching Bai Yi, “Research on the Security Model for E-business Management,” Published in IEEE computer society, 2009.
2. LI Yuiwin, “Research on E-commerce Technology,” Published in IEEE computer society, 2011.
3. Yuaquao Zen,Chuhui Zhou,Kezhong Liu,“Research on E- commerce Security Problems,” published in International Seminar on Business and Information Management, 2009, pp.186-189.
4. Hie Yu, Jiag Juan, “E-commerce Secur ity Payment System Research and Application ,” Published in IEEE Computer Society, 2011, pp.559- 562. [online] **http:/ / www.ecommerce-digest.com/ 79.html.** (Accessed 23 Sept 2013).
5. Geng Li-xiao, Zeng Zhen-xiang,Zhang Xue-min,“Research on PKI based E-commerce security Mechanism,” Published in IEEE conference, 2007, pp.3545-3547.
6. Dai Wei, Ji Wei, “Research on the Security of an improved E-commerce Model,” Published in International Conference on E-Business 2010.
7. E-commerce and Development Report By United Nations Conference on Trade and Development, 2002.
8. Richard Gay, Alan Charlesworth, Rita Esen, Online Marketing: A Customer -Led Approach, 2007.
9. Seyyed Mohammad Reza Farshchi, Study of Security Issues on Traditional and New Generation of E-commerce Model IPCSIT vol.9.
10. Thulasimani Lakshmanan and Madheswaran Muthusamy, “A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes” The International Arab Jour nal of Information Technology, Vol. 9, No. 3, 2012.
11. Dr.Nada M.A. Al-Slamy, “E-commerce security” IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, 2008.
12. Rhavani Chris Clifton, “Directions for Web and E-commerce Applications Security” ISSN 0-7695-1269-0101 1-2001, 2001.