Cryptography final submission

by Dhruv Maheshwari

Submission date: 19-May-2022 08:22PM (UTC+0400)
Submission ID: 1839937825
File name: Cryptography_final_submission.pdf (549.59K)
Word count: 2532
Character count: 13137

BITS Pilani
Dubai Campus

Prevention of Online Frauds

Using cryptographic approach

Adaya Neeraj, Dhruv Maheshwari

Acknowledgment

We owe a great many thanks to a great many people who helped us in this project.

Our deepest thanks to the project supervisor Dr. Raja for giving me this opportunity to do this knowledge-full project and keep his faith in us and supporting us throughout the project and giving us motivation and inspiring us to be more creative.

Also, we want to offer our ardent thanks to the Director of BITS Pilani, Dubai Campus, Prof. Srinivasan Madapusi, who has always guided us towards the right path.

Index

Abstract

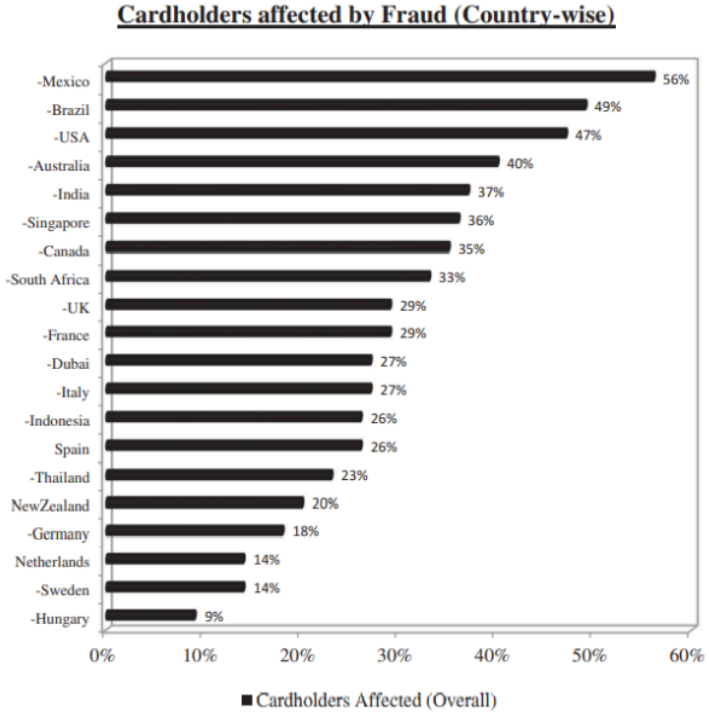
With the technological advancements in the 21st century and the age of globalization, traditional banking system is slowly being replaced by online banking. People use this service to conveniently send funds across the globe, buy goods from e-commerce websites, pay their bills etc all with a simple touch on their gadgets from the comfort of their home. People seldom realize that their passwords, card information and other sensitive information may get compromised and they may become a prey to online fraud. This study evaluates current algorithms in place to counter online frauds and also tries to suggest an algorithm to further improve the strength of these algorithms.

Introduction

Confidentiality, integrity, and availability are the three security principles that must be considered in any cyber-related operation. The safeguarding of sensitive information from unauthorized access is referred to as “confidentiality”. The term "integrity" relates to the data's accuracy and dependability during the course of a transaction The term "availability" refers to the ability to complete a transaction without the system failing.

Although all financial institutions adhere to these security procedures, cyber criminals, i.e., fraudulent people, compromise the certainty (confidentiality and integrity) by compromising the credit / debit cards which are used for transactions. These types of frauds takes place from the user's side, where fraudulent people steal information and gain unauthorized opportunity to use the user's account by posing as a legitimate consumer.

According to the numbers, Mexico is the most seriously impacted country, with around 56 percent of card holders being victims of fraud; India is in fourth place with a fraud rate of 37 percent; and Hungary is the least afflicted country, with a fraud rate of 9 percent (Kiernan 2016). Fraud affects all major countries which includes “The United States”, “The United Kingdom”, “Australia” and “France”.



There are two types of approaches for authentication:

1. Single Factor Authentication:
   Only a password is used for logging in, transacting etc.
   It has serious drawbacks:

The user may use the same password for multiple accounts. If the attacker gets his hand over the password, the security of all the accounts would be compromised.
Even when user has different passwords for different accounts, weak passwords can easily be cracked using brute force approach.

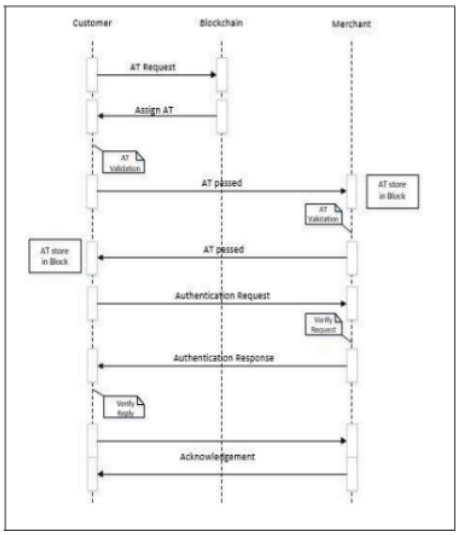
Web banking systems, like any other web application, transport data via the Hypertext Transfer Protocol (HTTP). All communications involving data movement over HTTP must be secure. Because the POST method is more secure than the GET method of HTTPS, the Secured Socket Layer (SSL) or Transport Layer Security (TLS) protocol (i.e. HTTP Secure over SSL or HTTP over TLS (HTTPS)) must be used when delivering data.

2. Multi-Factor Authentication:
    - Knowledge (First factor: what you know): It is asked at the time of authentication from user. Eg- PIN, password etc.
    - Possession (Second factor: what you have): Eg- OTP, security tokens, mobile authentication.
    - Inherence (Third factor: who you are): Verifies physical existence of user. Eg- biometric recognition
    - Location (Fourth factor: where you are): Uses GPS to tell from where the transaction was initiated
    - Time (Fifth factor: when): Uses timestamping to systematically store record of transaction.

This research focuses on online payments made with a debit or credit card or through net banking or any kind of online payment. The threat lies on the user's side in such situations and not at the end of the financial institution or in the mechanism through which the attributes are conveyed to these institutions. The study aims to find a novel solution to lessen the rate of deceitful transactions and safeguard millions from scamsters.

Literature Review

According to Maria Rona et al, the use of blockchain technology can help in securing the sensitive payment information. They have worked on modifying SHA256 and create a robust security system backed by blockchain mechanism. According to them, both seller and consumer should register on Blockchain. Once registered, the server would send tokens to both the parties and once the tokens are received, both can communicate with each other securely.



Blockchain uses SHA256 hash algorithm. A customized token in a new block (nVer) composed of a previous block (HPrB), hash values and nonce (N). A key resolver is used for two sign tokens carrying the timestamp, where verification and authentication happens.

The initial connection requires permission from blockchain. Decryption at the blockchain happens with the private keys of seller and customer along with the shared token. The blockchain then encrypts and forwards the data with its own private key.

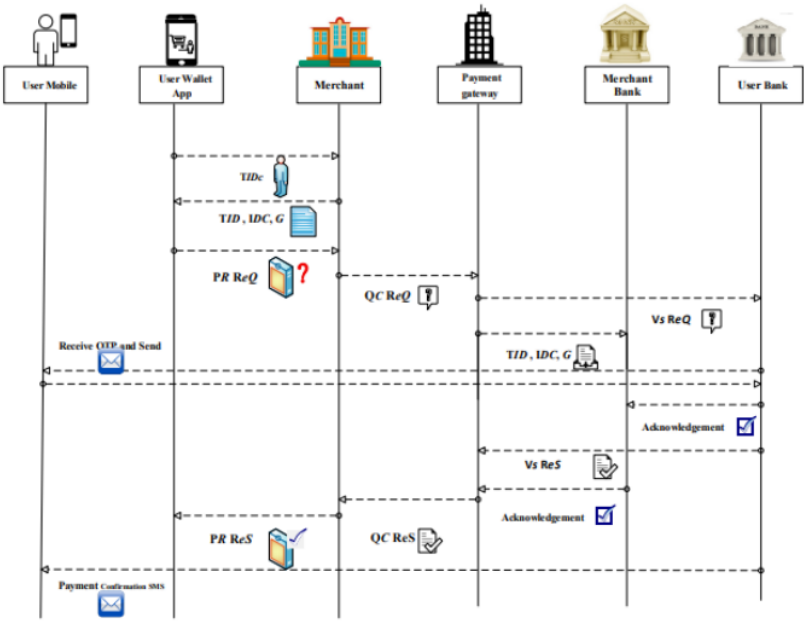
Once a connection is established, the entities use their private key and other's public key to encrypt and decrypt the data.

In methodology proposed by Md Arif Hassan et al, they work on existing RSA model to increase security. They also claim to hide the identity of the customer and the customer can access the seller website using a temporary identity. Izhar et al used Triple Data Encryption Standard (TDES). They designed a system to give a reliable electronic payment portal ensuring authorization, integrity, confidentiality and availability. However, they didn't address non-repudiation and anonymity.

The consumer, seller, consumer and seller account, all register with payment portal to create their own unique key with it. The consumer and seller have an exclusive key between themselves.

TIDc—temporary identification of client
IDC—the identity of the product
G—goods details including price, date, and transaction identification
QC ReQ—value claim request
QC ReS—value claim response
PR ReQ—product request
PR ReS—product response
Vs ReQ—value subtraction request
Vs ReS—value subtraction response

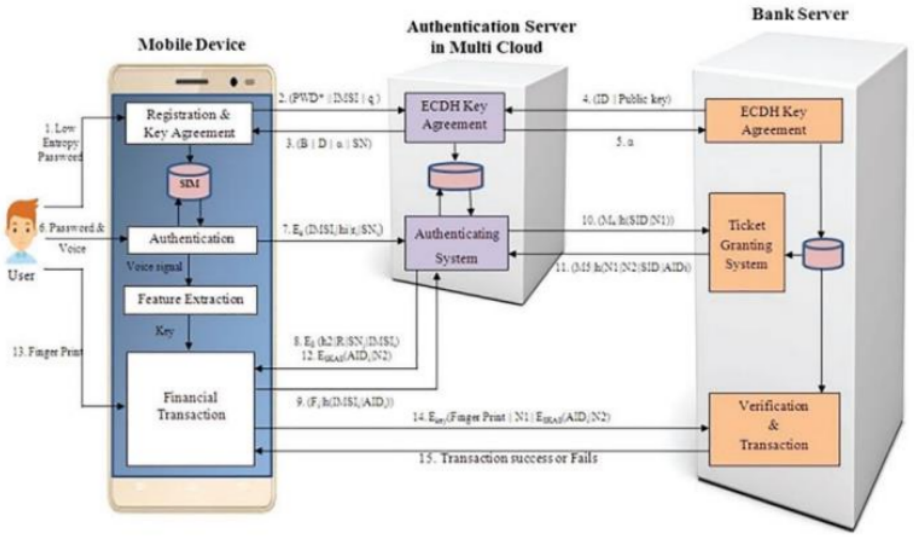
A detail explanation of the process is provided below; "Alice' → Bob: C" indicates a message C is delivered to Bob by Alice. The proposed transaction protocol phase is presented in Figure 4.



In this, the user masks his original identity and places an order on the e-commerce. All the transaction details are encrypted using RSA architecture. Once order is placed by consumer, the seller sends value claim request to payment portal. At the same time, payment portal sends cost of goods to the seller bank. Payment portal also send value reduction call to consumer bank. Consumers' bank sends OTP for verification. Upon successful verification, consumer bank sends value reduction feedback to payment portal and seller bank also sends an acknowledgement. The value claim response is sent to seller from portal which in turn confirms that order has been placed successfully to the consumer.

Another paper suggests a framework with Multifactor Authentication (MFA) using low entropy password with voice recognition, the references and session key are encrypted using "Elliptical Curve Cryptography (ECC)".

The proposed architecture has 5 phases, account registration, user verification, voice coefficient extortion using "Mel Frequency Cepstrum Coefficient (MFCC)", session key generation and shielded transaction phase.



The user accesses bank using less informative password and voice. The user registers with authentication server using a less informative password and "International Mobile Subscriber Identity (IMSI)". Bank registers using a key pair. The authentication server is supposed to verify the user details and upon verification, the authentication server passes the same permit to user that it was provided from the banking server.

Problem Statement and Possible Solution

Problem Statement:

As the amount of people transacting online has risen exponentially over the years, so has the number of frauds. We aim to suggest a model that verifies the user and has a secure communication algorithm between the user, seller, users' bank, seller's bank and payment portal.

Possible Solution:

For user authentication, it is important that we capture biometric information such as voice and fingerprint. The algorithm can also capture mobile IMEI number, geolocation (which can't mask location even if attacker is using a VPN) and timestamping may be done to ensure the packets are destroyed once their useful life is over.

A third party, a portal or a server in place can monitor transactions between various entities and abort the transaction in case of any suspicious activity. All the cryptography process must be done using asymmetric key, must use RSA or ECC.

Proposed Algorithm

In our proposed scheme, we would be having 4 members: client, bank, shop/website/merchant and trusted third party (TTP).

When a client places an order, he would request for a payment voucher from his bank. Upon receiving the voucher, the client would create a Digital Signature (DS) and forwards the encrypted DS to the seller. After verification of the packet, the seller confirms the order to the user. The user then sends the payment voucher to the seller. The seller sends it to the bank before expiry time and the money is deposited into seller's account. If there's any discrepancy in any of the transaction, TTP steps in to resolve the issue.

The process would be having 5 phases

1. Initializing phase
    - Field F is selected st $p \geq 2^{160}$ and an elliptic curve (ECC) E_p (a, b).
    - Base point G is selected and symmetric key encryption E_k and decryption D_k
    - Each member with id ID_i calculates private key d_i and public key $Y_i = d_iP$
2. Buying phase
    - User U gets good info I from website.
    - Selects $r \in Z_q$, calculate $A = r(d_u + T_1)$ {T_1 is the time stamp}
    - $K = rY_b = (k_x, k_y)$
    - p = price of goods
    - $m = I \| p \| ID_b$
    - $C = E_{kx} (ID_u \| m \| p \| k_x \| T_1)$
    - (ID_u, C, A, T_1) is sent to the bank
3. Paying phase
    - Bank B computes $K = A(Y_u + T_1P)d_b = (k_x, k_y)$ ----- (1)
    - Decrypts C by D_{kx} (C) = $(ID_u \| m \| p \| k_x \| T_1)$ ----- (2)
    - Authenticates k_x is same in (1) and (2) and validates T_1. In case of any error, it rejects the process.
    - Post verification, bank deducts amount p from users account and stores it with itself.
    - M = m ‖ E is computed where E is expiry and M's DS is created based on ECC and stores (M, DS) with itself.
    - $C = E_{kx} (E \| DS \| T_2 \| k_x)$ is sent to user {T_2 is timestamp}
4. Exchange phase
    - $D_{kx} = (E \| DS \| T_2 \| k_x)$, DS and E are obtained. r', $z \in Z_q$, A' = r'P, Z = zP
      K' = r'Y_m = (k_x', k_y')

$C = E_{kx}$' (DS' || E || ID_b || I || T_3 || k_x') { DS' is a verifiably encrypted digital signature obtained by using random number z, K_{TTP} and the DS}
Merchant M receives (C, A', Z, T_3) from U

- M calculates K' = d_mA' = (k_x', k_y') and decrypts C using k_x' to get (DS' || E || ID_b || I || T3 || k_x'). Authenticates k_x' and T_3.
  M calculates p and m = I || p || ID_b and M = m || E and verifies DS'.
  If everything is in place, M sends confirmation C = E_{kx}' (message) to U otherwise it terminates the transaction.

- U receives C, obtains the acknowledgement message and sends C = E_{kx}' (DS) to M
  M obtains DS and verifies it.

5. Transferring phase

   Merchant sends DS to bank and bank verifies with (DS, M) stored with it. If match is found, money is transferred into merchants account and bank removes (DS, M) from its database.

Conflict Removal Phase

If M doesn't get DS after sending acknowledgment to U, M can show (DS' || I || T_3 || Z || E) to TTP. TTP would calculate p, m = I || p || ID_b, M = m || E and verifies DS'. If valid, TTL computes DS using his private key from DS'. He gives DS to merchant and stores (DS, I)

If U doesn't get required I from merchant, user shows DS to TTP and if valid, TTP gives user I.

Discussion and Results

Our algorithm provides Anonymity and Fairness and ensures mutual authentication, confidentiality, integrity, resist replay attack and double spending attack as well.

All the messages which are transmitted include the time stamps which in the encrypted part cannot be altered hence the algorithm resists replay attack. Similarly, when a user sends good information (request) protected by one hash function to a bank and the digital signature does not reveal the user's information hence protecting the user's privacy and once the payment is transferred to merchants account the digital signature is deleted by the bank hence it can be used only once ensuring double spending attack.

While in case of anonymity and fairness the user's identity remains unknown to the merchant and since the bank only keeps the merchant's digital signature in their database it cannot trace the user who drew the digital signature from it during the transferring phase, keeping the anonymity of the user intact.

The algorithm is more complex, involves more timestamping and hence is secure than SHA256. However, a trade-off exists as with increased complexity comes increased computational cost.

Conclusion

The proposed algorithm satisfies anonymity and fairness properties which is not effective in other algorithms including the dispute resolution means. This algorithm is more secure and suitable for resource constrained environments and with the rapid development of information and communication technologies purchasing through the internet has been greatly increased. Hence increasing requirement of more secure environments.

With the era of digitalization, there is a boom in number of electronic payments being made. The principal issue remains finer need for a reliable payment system and online authentication at the consumer side. An algorithm should be smart enough to distinguish between a genuine and illegitimate user and also provide a secure way of transacting using bank details, debit/credit cards or QR based payments. The algorithm must possess confidentiality, non-repudiation, integrity, availability, and anonymity to continue the faith of people in e-banking.

References

1. A. Hammood, Waleed & Abdullah Arshah, Ruzaini & Hammood, Omar & Mohamad Asmara, Salwana & Al-Sharafi, Mohammed A. & Muttaleb, Ali. (2020). A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number. IOP Conference Series: Materials Science and Engineering. 769. 012061. 10.1088/1757-899X/769/1/012061.
2. B. U. Islam Khan, R. F. Olanrewaju, F. Anwar and M. Yaacob, "Offline OTP Based Solution for Secure Internet Banking Access," 2018 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), 2018, pp. 167-172, doi: 10.1109/IC3e.2018.8632643.
3. K. Fan, H. Li, W. Jiang, C. Xiao and Y. Yang, "Secure Authentication Protocol for Mobile Payment," in Tsinghua Science and Technology, vol. 23, no. 5, pp. 610-620, Oct. 2018, doi: 10.26599/TST.2018.9010031.
4. Vipin Khattri & Deepak Kumar Singh (2019): Implementation of an Additional Factor for Secure Authentication in Online Transactions, Journal of Organizational Computing and Electronic Commerce, DOI: 10.1080/10919392.2019.1633123
5. M. R. L. Perez, B. Gerardo and R. Medina, "Modified SHA256 for Securing Online Transactions based on Blockchain Mechanism," 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), 2018, pp. 1-5, doi: 10.1109/HNICEM.2018.8666341.
6. Hassan, M.A.; Shukur, Z.; Hasan, M.K. An Efficient Secure Electronic Payment System for E-Commerce. Computers 2020, 9, 66. https://doi.org/10.3390/computers9030066

Cryptography final submission

ORIGINALITY REPORT

16%	3%	15%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Baoyuan Kang, Dongyang Shao, Jiaqiang Wang. "A fair electronic payment system for digital content using elliptic curve cryptography", Journal of Algorithms & Computational Technology, 2017 Publication	8%
2	Vipin Khattri, Deepak Kumar Singh. "Implementation of an Additional Factor for Secure Authentication in Online Transactions", Journal of Organizational Computing and Electronic Commerce, 2019 Publication	2%
3	umpir.ump.edu.my Internet Source	2%
4	Maria Rona L. Perez, Bobby Gerardo, Ruji Medina. "Modified SHA256 for Securing Online Transactions based on Blockchain Mechanism", 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and	2%

Control, Environment and Management (HNICEM), 2018
Publication

5	www.coursehero.com Internet Source	1 %
6	www.techscience.com Internet Source	1 %
7	D. Prabakaran, Shyamala Ramachandran. "Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment", Computers, Materials & Continua, 2022 Publication	<1 %
8	www.mdpi.com Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		