IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 3, 2021, accepted January 9, 2022, date of publication January 20, 2022, date of current version January 28, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145030

Secure E-Commerce Scheme

SENA EFSUN CEBECI, (Graduate Student Member, IEEE), KUBRA NARI, (Graduate Student Member, IEEE), AND ENVER OZDEMIR, (Member, IEEE)
Informatics Institute, Istanbul Technical University, 34467 Istanbul, Turkey
Corresponding author: Sena Efsun Cebeci (cebeci15@itu.edu.tr)

ABSTRACT E-commerce security has recently been an emerging topic due to the escalation in credit card fraud and stolen user accounts. In general, the security bridge and privacy leakage occur on the side of e-commerce companies due to various factors such as flaws in the design of their storage systems. The stored information of users increases the risk on privacy bridge and to remedy such risks e-commerce companies are forced to make costly investments. The security threats also enforce the development of robust security protocols and methods in digital commerce systems. The current protocols and methods generally bring extra communication and computation costs to all parties involving in the e-commerce system and the security risk on the side of e-commerce companies still remains. In this paper, we propose a Secure E-commerce Scheme (SES) which alleviates the security threats on the side of e-commerce companies and reduces communication costs for all parties. The proposed secure e-commerce protocol, SES, is implemented, analyzed and compared to two well-known schemes; Secure Electronic Transaction (SET) and 3D Secure.

INDEX TERMS E-commerce security, security protocol, algorithm development, symmetric key cryptography.

I. INTRODUCTION

The increase in credit card fraud and stolen user accounts aroused considerable interest among information security community to take precautionary steps for the e-commerce system. Recently, it has been reported that hackers have stolen 143 million US customers' personal data including credit card information from Equifax [1]. The most critical security problems that are known to exist in e-commerce are the credit card fraud and the compromising of the users' account information. The reasons for such security issues are due to several factors. The most problematic one is keeping personal information as a plaintext in any database. Even storing personal information in an encrypted format does not remove the security concerns as the culprits for the majority of bridges are insiders [2]. In fact, most of the stolen data from e-commerce companies was already kept in an encrypted format. For example, Alibaba, a well-known online shopping website, was compromised in 2016 and 20 million user accounts were stolen [3].

Over the course of last 20 years, the number of people using online tools for shopping has been increased along with the security and privacy concerns [4]. Due to recent precautions to prevent the spread of corona viruses, online shopping has become an indispensable part of our daily life [5]. E-commerce companies have developed several tools and methods to make online shopping as easy as possible. In this respect, an e-commerce company stores customers' credit card information and address to avoid requesting the same process from a customer for each transaction. Users' credit card information might be stored in the system as a plaintext or as a ciphertext via a known encryption method. Even if users' data is encrypted before it is stored, the security of it still cannot be fully provided. For instance, a system administrator from the e-commerce company or anyone who has all the access privileges can easily decrypt the stored data and use it for malicious purposes. Keeping customers' information in their database makes e-commerce systems targets to hackers and taking necessary measures to prevent attackers from obtaining private information puts an enormous burden on these companies. The measures in general require installment of costly hardware systems along with software. Therefore, the main motivation for the research community is to create an online shopping scheme which is user-friendly and at the same time respectful to users' privacy. In addition, the scheme should reduce the risk on e-commerce companies, so that they will not have pressure to make costly investments to

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Aljawarneh.

secure their systems. With this motivation, several security algorithms (Secure Sockets Layer (SSL), Secure Electronic Transaction (SET), 3D Secure, Two-factor Authentication etc.) have been added to online shopping tools recently [6]–[10]. On the other hand, these security add-ons have no significant effect on reducing the pressure on e-commerce companies. The objectives of such tools in general provide confidential and authenticated data transaction between all parties involving in an online shopping. For example, SSL protocol is designed to ensure confidentiality, end-points authentication and integrity in transport layer. The SSL scheme applies public key algorithms, however the protocol comes with a high communication and computational costs [6]. A standalone e-commerce protocol, SET, which is used in practice for secure e-commerce, is constructed especially to protect users' privacy [8]. The method still comes with a great communication load, requires re-entrance of users' data and includes a relatively long preparation phase. In addition to aforementioned protocols, 3D Secure method which mainly focuses on verification of users during the transaction has been introduced recently [9]. This method applies two-factor authentication by certifying each user with a prechosen password and a one-time authorization code produced by the bank while the online transaction is being processed [10]. The issue of communication costs and storing users' data on e-commerce side still remain in this approach.

In this paper, an online payment scheme is presented to remove security concerns on the private data stored in e-commerce companies' databases while still allows user-friendly online shopping environment. A brief summary of the contribution is stated below.

A. CONTRIBUTIONS OF THE PAPER

The proposed scheme:

- Provides a secure e-commerce protocol assuring that users' sensitive information cannot be extracted in case the e-commerce company's database is compromised.
- Preserves users' privacy with the data manipulation technique used in the protocol and eliminates the users' concerns on the protection of their data in the e-commerce company's data storage.
- Reduces the costs of securing the data storage systems in e-commerce companies.
- Removes the necessity of re-entrance of the user information in each transaction.

The remaining of the paper is structured as follows. The following section is devoted to related work in this research area. In Section 3, mathematical structures of the proposed protocol are introduced. The detailed explanation of the protocol is presented in Section 4. The security analysis, evaluation and the experimental results take part in Section 5. The final part, Section 6, includes conclusion and recommendation of a future work.

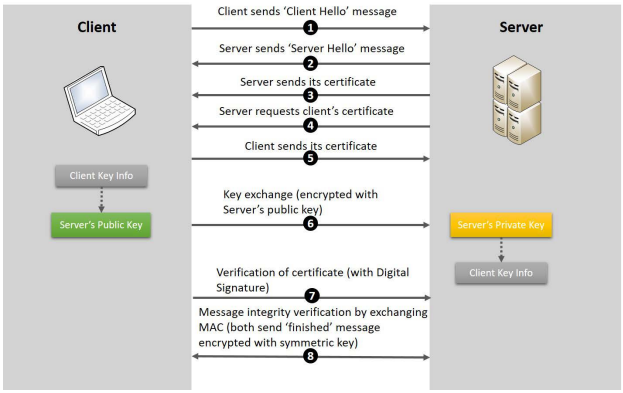


FIGURE 1. Secure Socket Layer (SSL) life cycle.

II. RELATED WORK

Security requirements in digital communication known as confidentiality, integrity and availability of data should be fulfilled in an e-commerce system as well. For this reason, several security protocols and algorithms for secure online transactions are presented [11]–[17]. Various security issues arose while implementing online transactions [18]. For example, replay attacks [19] which means an attacker performs the same online transactions on behalf of a legitimate user, were conducted frequently in the past. Security measures are costly in terms of monetary and time. For example, even the least costly measure to provide confidentiality of data transaction between a legitimate user and the e-commerce company requires a strong authentication algorithm, a secure key exchange method and a standard data encryption technique. Even though these costly measures are taken all together by e-commerce companies, banks and EMV (Europay, Mastercard and Visa), there are still security issues which should be addressed. In this section a brief description of currently used measures is presented.

Secure Sockets Layer (SSL) [6] was first introduced to relieve security concerns at the transportation level in computer networks, however it becomes indispensable add-on for secure online transactions [7]. In SSL protocol which is depicted in Fig. 1, the credit card owner's information is encrypted then sent to the e-commerce company [20].

All exchanged data is encrypted with a key agreed by the user's application (i.e., web browser, mobile application etc.) and the e-commerce server, in this way the data flowing in an open channel stays confidential. The agreed key is exchanged via Rives-Shamir-Adleman (RSA) public key algorithm [21]. The SSL add-on the transportation control protocol (TCP) increases communication and computational costs for both parties. Due to the design of SSL, certain disadvantages should be expected, such as speed degradation [22]. Former versions of SSL protocol are vulnerable to certain attack types. For example, SSL 1.0 is defenseless to replay attacks [23], for SSL 2.0 only one public certificate is provided and some keys for message authentication and encryption cause security problems [24]. Furthermore, MD5 (Message Digest) [25] hash function is implemented on SSL

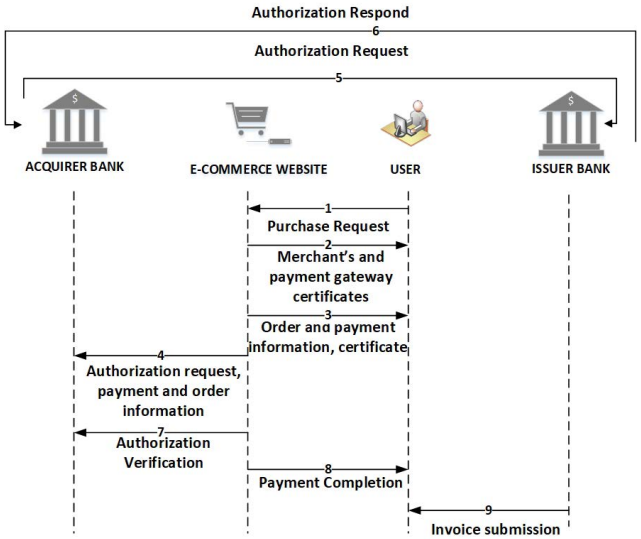


FIGURE 2. SET protocol transaction flow.

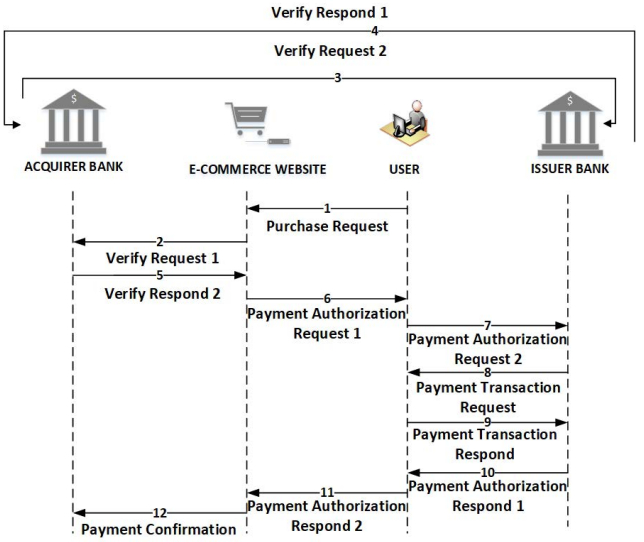


FIGURE 3. 3D Secure method diagram.

2.0 that is known to be prone to hash collision weakness [26]. In later version of this protocol replaces it with SHA-1 (Secure Hash Algorithm 1) [27] as a hash function. However, SSL 3.0 is reported to be unguarded to POODLE (Padding Oracle On Downgraded Legacy Encryption) attack and also hash collision is detected in SHA-1 [28].

In early 21st century, a new protocol called Secure Electronic Transaction (SET) for secure online shopping was introduced [8]. The protocol's aim is to remove the necessity of keeping users' credit card information from e-commerce companies. Fig. 2 illustrates the operations in payment transaction of SET protocol.

Transactions' privacy is protected from adversaries in online secure environment with a virtual wallet and a certificate. On the other hand, the company can still access user's credit card information. Therefore, the method still holds pressure on the e-commerce side to take precautions for the security of its data which makes customers reluctant to share their information. SET protocol guarantees that payment information is confidential during the online shopping process. In addition, it authenticates the card user and establishes an agreement between e-commerce company and the bank [29]. Like SSL, SET also requires confidential communication between all parties. The confidentiality of the transactions is fulfilled via employing a symmetric key and a public key algorithms. In order to benefit from this system, the credit cards must be compatible with SET protocol. To comply with SET protocol, each credit card must be certified by a Certification Authority (CA). Moreover, the credit card holders should have a virtual wallet in his/her computer which is provided by the issuer bank and the virtual wallet must be included with SET certification. Purchases can only be made from SET-compatible companies with the virtual wallet. Even though SET protocol provides higher security than SSL, the failure to become widespread for e-commerce systems may be due to the lack of mobility of the virtual wallet. Furthermore, the requirement of re-entering credit card information for each transaction causes another drawback for the popularity of this protocol [29].

Apart from SSL and SET protocol, to increase security level, certain online shopping applications require Payment Card Industry Data Security Standard (PCI-DSS) certification [30] or additional authentication methods like 3D Secure [9], [31]. 3D Secure method is widely accepted and adapted by the banks and e-commerce companies. The method is designed especially to prevent shopping with a stolen credit card. In order to ensure the card holder's identity in payment process, 3D Secure method forces banks and e-commerce companies work in collaboration. In other words, during the payment process, a special 3D transaction authentication application runs on both bank's side and the user's side. The bank provides a confirmation code to the user via short message services (SMS). Payment process can be completed upon user's code is confirmed by the bank. The complete shopping process includes at least two times authentication of the credit card user. In the first time, the user and the card information should be provided to e-commerce company and then confirmed by the bank. The second authentication is performed by the bank and e-commerce company via bank provided one time code to the user. These processes increase communication cost during an online shopping and they do not remove the necessity of e-commerce companies of storing users' information. Therefore, the scheme increases communication burden of e-commerce company and it still doesn't remove the pressure for securing user's private information on the e-commerce company. The life cycle of a single payment process with 3D Secure method is depicted in Fig. 3.

In tokenization method [32], in order to preserve the user's data security a unique digital value called 'token' is used instead of user account number. However, generating tokens and processing them during the transactions bring additional

costs. In addition, the method is vulnerable to replay attacks as the tokens can be reused for later transactions. The token is only for concealing the actual credit card number and the e-commerce company still acquires users' other information. In addition to above secure online payment schemes, several other studies were conducted while especially focusing on authentication of parties in e-commerce systems. For example, the blockchain technology based authentication algorithm is presented by [33], [34] and IoT-based e-commerce structure is described in [35]. A method for checking user's credentials during the electronic payment process with a predetermined identity aiming to resolve credit card fraud is described in [36].

Another algorithm, similar to tokenization method, is proposed to carry out secure e-commerce transactions using a payment account number instead of the actual credit card information [37]. In this method users' encrypted data is stored in e-commerce companies' database. The users have no control over this data and security dependence on the e-commerce system still exists. Ginter et. al. presented methods and technologies for electronic rights and management support services to provide efficient management and communication in e-commerce [38]. In this paper, security, validation and verification issues are handled and the well-known cryptographic algorithms such as RSA, El-Gamal public key are utilized. The method mainly focuses on the confidentiality of data transaction between parties instead of users' privacy.

The security bridges in e-commerce systems are mainly due to human factors. In other words, the problems occur not because a vulnerability of a cryptographic primitive, it occurs because of the design flaw in the system. The proposed method in our work is to remove the risks coming from malicious behavior in an e-commerce company side. Even though, there is various research conducted to detect malicious behavior in the e-commerce systems, still open issues exist to detect vulnerabilities. To this end, to identify the malicious behavior in an e-commerce system employing Petri nets are presented in [39], [40]. Wang *et al.* proposed a method using hidden Markov models to detect unobservable transitions in e-commerce transactions [39]. The method simply constructs a vulnerable e-commerce transaction net which implements labeled Petri nets, detects vulnerabilities and possible attacks, evaluates these vulnerabilities and attacks in the e-commerce system and prevents them before their occurrence. In [40], extended colored logic Petri nets' practicability ensuring the information security with strict conservativeness property for e-commerce systems is presented. E-commerce system is divided into different compositions namely a customer, a merchant and a third-party, extended colored logic Petri nets are implemented to each subdivisions and the properties of the proposed method are analyzed.

A machine learning method relies on boosting is proposed to identify transaction fraud due to distinct distribution nature of credit card transaction information in [41]. Experimental analysis indicating the performance of the method across various datasets is performed. Secure negotiation protocol for e-commerce is proposed in [42]. This work mostly concentrates on improving customer's utility in negotiation process of the transaction. The e-commerce system is based on multi-agents to preserve security and it is verified by experiments showing the robustness of the protocol to certain security attacks.

TABLE 1. Comparison of protocols.

Protocol Name	Advantages	Disadvantages	The risk factor on E-commerce*
SET	- User authentication - E-commerce authentication - Data integrity	- Requirement of SET compatible credit card - E-wallet requirement on users' side - Communication cost - Certification load	Exist
3D Secure	- Two-way authentication - Bank confirmation of purchase - Data integrity	- Communication cost - Adaption of users to the process - Certification cost	Exist
SES	- Protecting users' privacy - Performance - User-friendly	- Computation load on bank side - Certification cost - Communication cost	Non-exist

* The risk factor on e-commerce side indicates the possibility of stealing users' information from e-commerce databases.

The proposed method in this paper is inspired by the well-known problem of secret sharing in cryptography. Similar to any secret sharing algorithm [43], [44] user information is split into shares and only if enough shares available then the user information can be compromised. In some sense our method distributes the user information to the system actors which are the user, the bank and the e-commerce company. For instance, the e-commerce company database stores the manipulated user information and the bank provides a token which is time dependent and it is necessary for the e-commerce company to authorize its transaction via bank and EMV. In other words, only when e-commerce company's certificate, the manipulated user data, the price information and the token are combined by the bank, then the transaction can be authorized. On the other hand, unlike secret sharing algorithms, the proposed protocol does not employ a threshold mechanism. Comparison of SET, 3D Secure and proposed SES protocols and the possible risk that they put on the e-commerce side are given in Table 1.

Before presenting the details of the proposed method, the next section is devoted to a brief summary of mathematical building blocks of the algorithm.

III. MATHEMATICAL BACKGROUND

The confidentiality of data that flows in open channels is generally provided by a symmetric key algorithm. In a symmetric key cryptography, all communication parties should have the same secret key prior to the conversation. That is the stage where asymmetric key cryptosystem or in

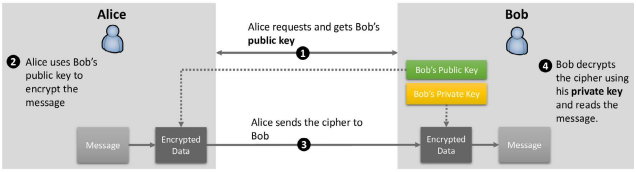


FIGURE 4. Public key cryptosystem.

strict sense a public key cryptosystem is employed. Even though Diffie-Hellman key exchange algorithm [45] is the first mathematical based asymmetric algorithm, several other asymmetric key algorithms are presented [21], [46], [47]. The majority of the algorithms employ certain multiplicative groups. Such an employment of a group is also exploited in the proposed algorithm.

Theorem 1: Let G be a multiplicative group of order n and 1 *be the identity element of G. Then for any* $a \in G$

$$a^n = 1$$

Proof: The theorem is due to Lagrange and the general statement of the theorem specifies that any subgroup of G has order dividing n [48]. □

Lagrange's Theorem has been utilized in many applications including some popular cryptographic algorithms, RSA and Elliptic Curve Cryptography [49]. The use of this theorem is coming from the observation that for any element $a \in G$, we have $a^{kn+1} = a$ for any positive integer k where again n is the order of G. A use of this observation can be illustrated with RSA algorithm. Let G be a group whose order n is only known by the receiver Bob. Bob broadcasts an integer e which is coprime to n. In other words,

$$\gcd(n, e) = 1 = ny + ex \text{ for some integers } x, y.$$

Lagrange's theorem 1 implies for any element a of G, a^n is the identity in G. In this respect,

$$a^{xe} = a^{1-ny} = a \cdot (a^n)^{-y} = a \cdot 1^{-y} = a \text{ in } G$$

In this process, Bob constructs his public information which is the group G and the integer e. Bob's private information is x and the group order n. Design of RSA algorithm ensures that the private information is hard to be found with the public data (G, e). In RSA algorithm, the group G is selected to be the multiplicative group modulo m, i.e., $G = (\mathbb{Z}_m^*, \cdot)$. In this design, the possible way to find Bob's private information is via factoring the integer m.

Alice, who is the sender, first downloads Bob's public information (G, e). Then, she represents her message as an element a of G. She obtains the cipher c by computing a^e in G. RSA is one of the most used public key algorithms in practice and the process of a public key cryptosystem is illustrated in Fig. 4.

The proposed protocol requires employing a symmetric key algorithm in one of the steps. A symmetric key cryptosystem is the oldest method providing confidentiality of

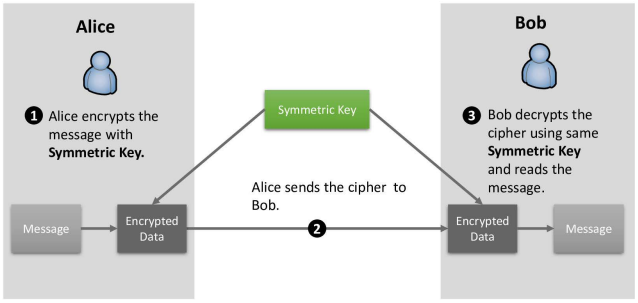


FIGURE 5. The work flow of a Symmetric Key Algorithm.

messages. In such a system the sender and the recipient must have a prior knowledge of a unique key which is used both with encryption and decryption functions. Even though in this digital era most of the systems utilize the standard symmetric key algorithm AES (Advanced Encryption Standard) [50] (previously DES (Data Encryption Standard)) [51] and its derivatives, certain systems employ non-standard algorithm. The following Fig. 5 depicts the work flow of a symmetric key algorithm.

IV. SECURE E-COMMERCE PROTOCOL

In the proposed protocol, the aim is to provide a secure e-commerce scheme between all parties involving online shopping which are in general a user, an e-commerce company, a bank and an EMV. Current methods for online shopping are vulnerable to various cyber attacks. Recently, several e-commerce companies' systems have been compromised which jeopardize private information of millions of customers. Even though many e-commerce systems take costly measures including storing customers' information in an encrypted format, still several bridges in the systems have been reported each year. Compromising credentials of system administrators might result in disposing millions of customers' private information which was even stored in an encrypted format. This paper establishes a protocol which removes the necessity of obtaining users' information for the e-commerce companies and therefore the protocol alleviates the security risks on their systems.

The method offers a manipulation algorithm for the user data to be recorded in an e-commerce company's storage. The stored data can only be converted to the original one in a certain time frame with an additional data provided by the user. Fortunately, only the bank can transform the data to its initial form with the public certificate of the e-commerce company and the amount of transaction. Basically, in our scheme the sensitive user data is not stored in the online company's repository and besides, the user does not have to provide his/her all information to the company each time performing an online shopping. Thus, the user data can never be revealed by the company or the people who compromised the company's system. Before describing the details of the protocol, the parameters which will be used in the scheme are presented in Table 2.

TABLE 2. Protocol parameters and descriptions.

Parameters	Descriptions
D	Stands for the data consisting of the user's account number, e-commerce certification, and the user's personnel information such as address.
k	The secret key assigned by the bank which is used in a symmetric encryption algorithm.
D_0	Encrypted D under the symmetric encryption algorithm with k.
A	The total amount of money spent during a single online transaction.
T_n	The integer randomly generated by the bank for each frame determined by the bank.
$\mathcal{C}$	The encrypted data (the cipher).
uID	The unique number assigned to each user.
AHI	The account holder's information.
Enc	The encryption function.
Dec	The decryption function.

The presentation of the proposed protocol is divided into two parts. In the first part, the process which takes place during the first purchase is described.

A. THE PROCESS FOR FIRST PURCHASE

The first part of the protocol deals with the registration of a user to an e-commerce company's system. This process is performed only one time during the user's first shopping experience with the e-commerce company. At this stage, necessary user information like credit card number, billing address etc. and the certificate of the e-commerce company are combined by the bank. Let the combined data be denoted by D. The standard process between the credit card issuer bank and the responsible EMV is supposed to be performed as usual. This process includes sharing AHI (Account Holder Information) with the responsible EMV (Europay, Mastercard, Visa) by the bank. Note that an EMV works with the bank during the card verification process of the user.

The data D is encrypted using a symmetric key encryption method with a key k determined by the bank. For example, the AES algorithm might be employed. Let Enc be the encryption function, the encryption process returns D_0. In other words,

$$D_0 = Enc_k(D) \tag{1}$$

the resulting D_0 which is the manipulated version of D is sent to the user who conveys it to the e-commerce company. The process in this part is illustrated in Fig. 6.

Algorithm 1 The E-Commerce Scheme (SES) for Registration

Input: D
Output: D_0
2: **DataExchange**(D): User ↔ Bank;
1: **DataExchange**(AHI): Bank ↔ EMV;
3: $k \leftarrow$ **KeyGen**();
4: $D_0 \leftarrow$**Enc**$_k(D)$;
5: **Send**(D_0): Bank → User;
6: **Send**(D_0): User → E-CommerceCompany;

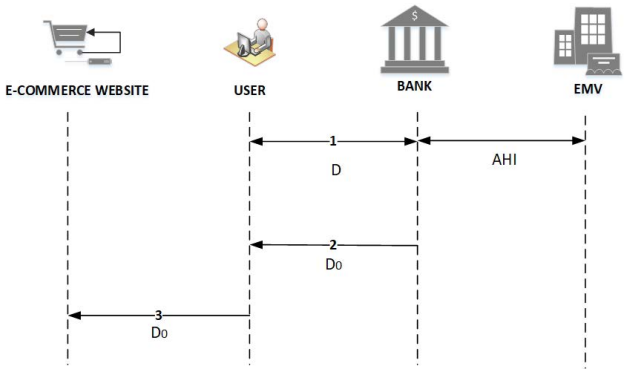


FIGURE 6. The first part of E-Commerce Protocol (First time user registration to the E-commerce system).

During the connection established between the user and the e-commerce system, the D_0 value is sent securely to be stored in the e-commerce company's database. Thus, the registration phase is completed. After the registration phase, the user does not need to enter the necessary payment information such as credit card information in his/her next shopping. At this stage, the capture of user data from the D_0 in the e-commerce company depends only on knowing the secret key k which was stored only in the issuer bank. Note that the certificate of the e-commerce company is embedded in D_0, the value D_0 can only be used by this company.

B. THE PROCESS OF FUTURE PURCHASE

In this part, a detailed description of processes performed by the user and e-commerce company during a future online shopping is presented. Let assume that the user is conducting n^{th} shopping with the company. Once completion of product selections, the user ends up with the payment step on the e-commerce site. The payment amount which is denoted by A is shared with the credit card issuer bank and EMV.

At this stage, the bank determines a T_n value which depends on when the transaction takes place and the assigned T_n value is valid for a period of time decided by the bank. The T_n value is an integer value that the bank generates randomly for each time period, and this value is the same for all users who perform shopping in that specific time period. For the sake of completeness, we employ a modular group $G = (\mathbb{Z}_p, \cdot)$ where p is a large prime integer in this step. Note that, a developer of the proposed protocol is allowed to use any group instead of a modular group as long as the discrete logarithm problem (DLP) is hard for the selected group. The variables T_n and the amount A should be adjusted to the selected group. Assuming the discrete logarithm problem is hard for the group $G = (\mathbb{Z}_p^*, \cdot)$, T_n, k and A values are concealed by the following process and the cipher text $\mathcal{C}$ is obtained.

$$\mathcal{C} = (T_n kA)^{uID} \mod p \tag{2}$$

The encrypted $\mathcal{C}$ is sent to the user by the bank. The user transfers the ciphertext $\mathcal{C}$ to the e-commerce site. The e-commerce company attaches $\mathcal{C}$ to previous stored D_0 and

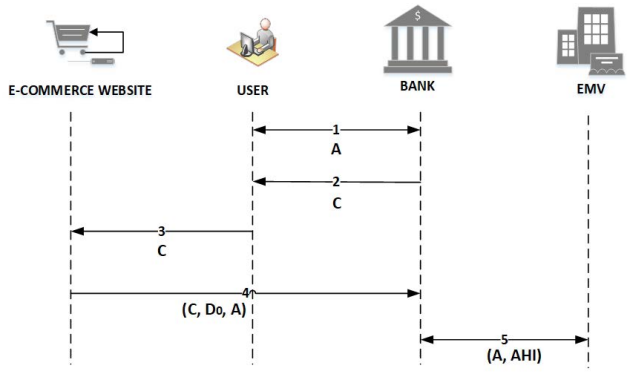


FIGURE 7. Secure E-Commerce Scheme (SES) diagram for round 'n' purchase and payment confirmation.

sends it to the bank along with A which is the amount information. The ciphertext $\mathcal{C}$ lies in a group $G = (\mathbb{Z}_p^*, \cdot)$. The group G has order $p-1$ which means that any element in G has order dividing $p-1$ by Theorem 1. In order to confirm the payment, the bank first determines an integer i such that

$$uID.i \equiv 1 \mod p-1 \tag{3}$$

Then, it computes $\mathcal{C}^i \mod p$ and gets:

$$\mathcal{C}^i = ((T_n kA)^{uID})^i = (T_n kA)^{uID.i} = T_n kA \mod p \tag{4}$$

Note that the above equation is coming from the theorem 1. In other words, since the group G has order $p-1$, for any element $g \in G$, $g^{k(p-1)+1}$ returns 1 for any positive integer k. Since we compute the number i so that $uID.i \equiv 1 \mod p-1$ which implies $uID.i = 1+k(p-1)$ for an integer k. This confirms $C^i = T_n kA$. The bank was the one who assigns T_n value and it has already received A from the user. Then it performs the following computation:

$$\ell = \frac{\mathcal{C}^i}{T_n A} \mod p \tag{5}$$

The ciphertext D_0 was obtained via an encryption function Enc. Then the bank decrypts D_0 with a decryption function Dec and the key ℓ that is

$$D' = Dec_\ell(D_0)$$

Once D' gives the user's information D, the bank confirms the payment via communicating with EMV. Note that encryption of D is via a symmetric key algorithm and therefore in essence the encryption function Enc and the decryption function Dec are the same functions. As long as ℓ in the equation 5 matches the original key k then the decryption function returns the user's data D.

The information $\mathcal{C}$, T_n, A and AHI should be confirmed between the bank and EMV for verification and payment confirmation. Actors and their behaviors in the system for online shopping data exchange depicted in the Fig. 7: Note that AHI is exchanged between the bank and EMV.

In summary, the first part of the protocol (Algorithm 1) deals with registration of a user to e-commerce systems in the first online shopping experience. The steps of this part:

Algorithm 2 SES Algorithm for Future Purchase

Inputs: T_n, k, A, uID
Output: $PaymentConfirmed \leftarrow True$ or $False$
1: **DataExchange**(A): User $\leftrightarrow$ Bank;
2: $\mathcal{C} \leftarrow (T_n kA)^{uID} \mod p$;
3: **Send**($\mathcal{C}$): Bank $\rightarrow$ User;
4: **Send**($\mathcal{C}$): User $\rightarrow$ E-CommerceCompany;
5: **Send**($\mathcal{C}, D_0, A$)): E-CommerceCompany $\rightarrow$ Bank;
6: Select i; $uID.i \equiv 1 \mod (p-1)$;
7: $\mathcal{C}^i \leftarrow T_n kA \mod p$;
8: $k \leftarrow \mathcal{C}^i/(T_n A) \mod p$;
9: $D \leftarrow Dec_k(D_0)$;
10: **DataExchange**(A, AHI): Bank $\leftrightarrow$ EMV;
11: **DataExchange**($Address$): Bank $\rightarrow$ E-CommerceCompany;

1) Sharing user data D between the user and the bank.
2) The bank exchanges and verifies the user information with EMV.
3) Bank generates a private key k for the user.
4) The bank generates D_0 by encrypting data D via a symmetric key algorithm and a secret key k.
5) D_0 is sent to the user.
6) The user sends D_0 to the e-commerce company and D_0 is stored in the e-commerce company's storage. By storing D_0, the e-commerce company is relieved to ask the user's information in future shopping.

The second part of the scheme (Algorithm 2) is related with exchanging data between the actors in later online shopping experience of the user with the e-commerce company. The actors and their tasks in the system for round $n (n \neq 1)$ and for different time frame T_n are presented below:

1) Sharing the payment amount A between the user and the bank.
2) The bank generates the encrypted text $\mathcal{C}$ from A, k, T_n, uID.
3) The bank transmits the cipher $\mathcal{C}$ to the user.
4) The user transfers the cipher $\mathcal{C}$ to the e-commerce company.
5) The e-commerce sends $\mathcal{C}$, D_0, A and its certificate to the bank. Confirmation of payment is performed by processing C, T_n, A with the steps 6-9 in Algorithm 2.
6) The amount A and the user's information AHI in the bank side are shared with EMV.
7) The final step in Algorithm 2 (Step 11) is optional and it might be in use in case a shipping information is needed by the e-commerce company.

V. SECURITY CHALLENGES AND SYSTEM EVALUATION

The current bridges in e-commerce system generally occur on the e-commerce companies' side. For example, most of the recent bridges which result in disposing of several million customers' data are all on the sides of e-commerce companies [2]. In addition, the current techniques employed in e-commerce system has certain security flows mentioned in the first part of the paper. These concerns put pressure on e-commerce companies to make tremendous amount of investments to protect their systems and customers' private information.

The proposed method aims to ease this pressure on e-commerce companies by establishing a new protocol. The resulting protocol allows manipulating user's data by the bank to be stored in the e-commerce companies storage systems. The manipulated data can only be converted to the original one by the bank in a certain time frame when the users are supposed to be conducting online shopping. This protocol removes the pressure on e-commerce companies' security concerns as well as it removes the necessity of re-entering users data each time conducting online shopping.

Moreover, the proposed protocol puts main burden on the bank side. The manipulation of users' data and the confirmation of payment via manipulated data are required performing computational tasks on the bank side. The cost of operations depends on the selected group G which was chosen to be a modular group based on a prime integer p in above illustration. The size of p should not be as large as in the case of Diffie-Hellman key exchange. In fact, in our algorithm, the group G is kept private by the bank and therefore the security of the systems would not depend on the hardness assumption of the discrete logarithm problem.

During the implementation of the proposed protocol, the cipher $\mathcal{C}$ and the manipulated data D_0 along with the amount information A from e-commerce system to the bank pass through a public channel. The first question is whether it is possible to obtain the private information of the user from D_0. D_0 is the encrypted version of the original data such that $D_0 = Enc_k(D)$.

Theorem 2: The stored information D_0 by the e-commerce company can be used to get the user information only if the presence of the secret key k.

Proof: The stored information D_0 is computed by the bank. The bank selects a suitable symmetric key algorithm and its encryption function is denoted by Enc. The user information D and the private key k are the inputs of Enc and the output is D_0. Therefore, in order to go back to D from D_0, it is necessary to posses the secret key k as in a symmetric key algorithm and the decryption function needs the same key as the encryption function. □

The above theorem points out that the only possible way to return back to D from D_0 is to get the bank's secret key k. The secret k is embedded into the cipher $\mathcal{C}$ that is $\mathcal{C} = (T_n kA)^{uID} \mod p$.

Theorem 3: The secret key k can be obtained from the cipher $\mathcal{C}$ if the group $G = (\mathbb{Z}_p^*, \cdot)$ and the bank's secret T_n are known along with the discrete logarithm problem in G is practical.

Proof: The secret key k is embedded to the cipher $\mathcal{C}$ via the operation;

$$\mathcal{C} = (T_n kA)^{uID} \mod p$$

The integer p must be known and $\mathcal{C}^{\frac{1}{uID}} \mod p$ must be computed to get $T_n kA$. Note that computing $\mathcal{C}^{\frac{1}{uID}} \mod p$ requires a practical method for the discrete logarithm problem in G. Even if all these (group information, DLP) are available, then obtaining the secret key k from $T_n kA \mod p$ still requires the knowledge of T_n. □

The cipher $\mathcal{C}$ is constructed by the bank which keeps the group information $G = (\mathbb{Z}_p^*, \cdot)$ and the time frame data T_n secret. Even though T_n stays the same for all users in a certain time frame it is kept secret by the bank. Let assume for a moment that, T_n is somehow known by an adversary along with the amount information A. Without group G, it is not feasible to make any operation to reach the secret k. Interestingly, if one assumes that G is also known then the adversary must know uID and solve discrete logarithm problem in G to reach the secret k. Therefore, obtaining the secret k is much harder than solving discrete logarithm problem in the group G. In summary, an adversary should be able to fulfill the following steps in order to reach users' information:

1) Obtain T_n.
2) Capture the group information.
3) Acquire the unique ID (uID) of the user.
4) Solve discrete logarithm problem in the group G.

In the following part, we present an analysis of the protocol against possible attack scenarios. The scenarios can be classified as compromising the database, replay attack and man-in-the-middle attack.

Attack Scenario 1: Compromise of E-commerce Database

1) The adversary accesses the database of the e-commerce company and downloads the manipulated data D_0 belongs to its users.
2) The adversary tries to extract D from the D_0.
3) $Dec_{Adv}(D_0)$ works only when the secret key k is available which belongs to bank. The adversary cannot resolve D_0 to get D.

   The above discussion indicates (Theorem V.1 and V.2) that the compromising the secret key k requires infeasible computational tasks. Therefore, the user privacy cannot be violated with compromising the database of the e-commerce company.

Attack Scenario 2: Replay Attack

1) The adversary employs a cipher $\mathcal{C}_{Adv} = \mathcal{C}$ where it was captured from earlier communication.
2) The adversary sends $\mathcal{C}_{Adv}$ to perform a replay attack.
3) The bank processes $\mathcal{C}_{Adv}$ but it does not reveal the secret k as T_n is valid for a specified time frame.

In addition to above attacks scenarios, an adversary might try to implement so called the man in the middle attack. As certification authorities were formed to remove such attacks, and the certificate of e-commerce company is already employed by the protocol this attempt cannot be successful.

The presented protocol provides a confident system which resolves the problems mentioned at the beginning of this section. For instance, the security of the proposed protocol is independent of the e-commerce company's system. Customer accounts and credit card information will never be captured even if the e-commerce system is compromised. Therefore, e-commerce companies will not have pressure on investing on security of their cyber systems. Furthermore, to avoid

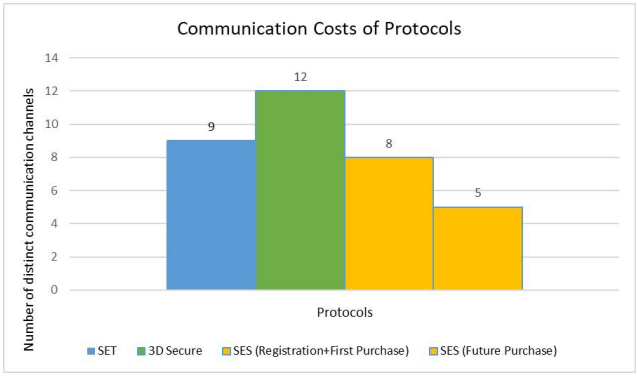


FIGURE 8. Protocols' communication costs: The number of communication channels generated by each protocol.

unauthorized transactions in the payment process, the protocol requires the user, the bank and the e-commerce company collaboration.

In addition, manipulated version of the user information that is stored in e-commerce company's database can only be decrypted with additional parameter gathered from the bank. In order to prevent any future dispute, SES algorithm requires confirmation from all parties; the user, e-commerce company and the corresponding bank. Therefore, in case of a dispute, the bank should be involved as it took a part in the confirmation phase and the bank can easily resolve the encrypted version of the user data.

The main advantages of the proposed protocol are as follows:

1) From the e-commerce company's point of view, encryption is not necessary while storing the received the banks' encrypted data about the user. Presented protocol eliminates the investment costs to keep the e-commerce system secure. Since only manipulated user data is stored in company's storage, a compromiser cannot obtain the user's private information with the captured data in e-commerce company side.
2) The application on the user side exchanges data with the bank and receives the manipulated user's information and it is convertible to the original data only by the bank. Therefore, users can be confident to use online shopping.
3) Compared to SET and 3D secure protocols, the online shopping process requires less communications in the proposed protocol. The registration part of SES is executed only once and the low number of communication channels during an online shopping in the scheme helps to reduce the network traffic. Communication cost of SET, 3D Secure and SES methods are shown in Fig. 8.

A. EXPERIMENTAL ANALYSIS

To illustrate the theoretical comparison mentioned in the previous section, we implement the well-known e-commerce security schemes, 3D Secure, SET and our method, SES. The test is conducted on a computer running on Linux operating system (Ubuntu 18.04) with Intel i7 5600U CPU and 8 GB memory. As for the software environment, Python 3.9 version is utilized along with the well-known Crypto library for Python, in particular we use Crypto.Hash (SHA1), Crypto.PublicKey (RSA), Crypto. Cipher (AES) which are all open to public [52]. The tasks while each of scheme is tested are explained in detail along with the average running time of each task in the next part. We should note here that all necessary communications for each of scheme take place inside of the computer.

1) TESTING SET PROTOCOL

We implement the following tasks for this scheme

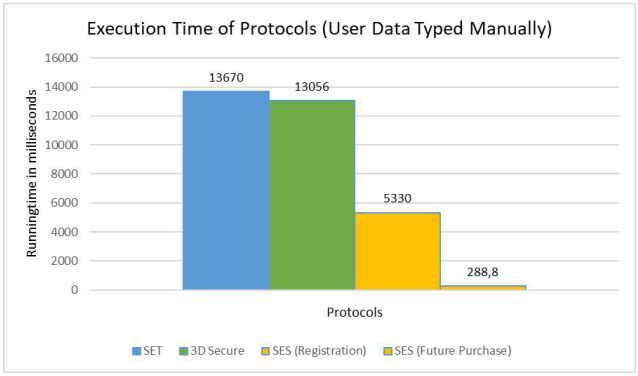
- KeyGeneration: This function generates public and private keys for each shopper.
- Encryption and Decryption functions for the public (1024 bits, RSA) and the symmetric key (AES256) algorithms.
- E-Wallet function which generates a random session key and shared with the bank by using the bank's public certificate. Another function called BankValidation also takes place to authenticate the bank. In other words, the bank should be able to decrypt the received session keys with using its private key.
- The last function, OrderConfirmation, is to verify the shopper's order by e-commerce company.

Note that, even though SET scheme requires entry of the shopper's credit card information for the payment, we first run the test without acquiring shoppers' information as we already embed such data to the source code. In other words, in the first part of the test, we embed user information to the source code and run the test for SET scheme. The average execution time for all processes is 3200 milliseconds. This average is obtained while performing the test for 100 times. In the second part, we test SET scheme by enforcing shoppers' to enter their credit cards information manually and the average time in this case is about 13670 milliseconds.

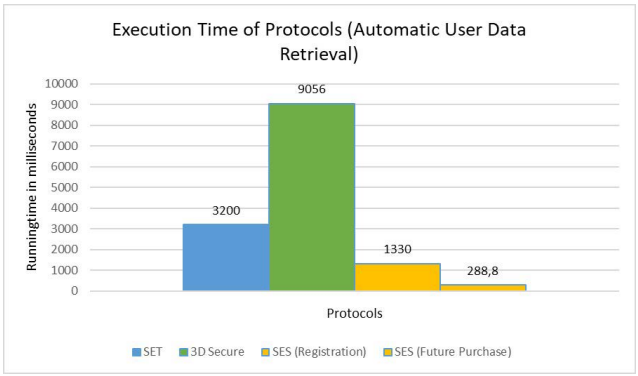
2) 3D SECURE PROTOCOL

The payment authentication process with 3D secure scheme includes acquiring the shopper's data (credit card, adress etc), but in our implementation as in the case of SET, we embed such data to the source code in order to evaluate solely the process running on each party (the shopper, the bank and the e-commerce company). The resulting time of the test is the whole executing time of the approval process of the payment. The whole process is combination of the following steps:

- UserAuthentication1 function which runs on the bank side to authenticate the shopper's information.
- UserAuthentication2 function which runs on the e-commerce company side to authenticate user via connecting VISA/MasterCard directory.
- ECommerceAuthentication function is to verify and exchange data between e-commerce company and the bank.



(a) Manual data entry



(b) Automatic data entry

FIGURE 9. Execution time comparison of the protocols with SES.

- OTPFuntion runs on the bank side to generate a key and sends it to the shopper for authentication of the final payment.

The above tasks are implemented with using Stripe application [53]. Even though the one time password (OTP) which is obtained via a short message service (SMS) is manually typed by the user in practice, we embed it to the source code in order to exclude the time spent by the user. The scheme is tested on the same hardware environment as in the case of SET for 100 times and the average running time is 9056 milliseconds. Note that, if the average time of typing OTP is assumed to be 4000 milliseconds then the average execution time of 3D secure becomes 13056 milliseconds.

3) SES PROTOCOL

We divide testing of our scheme into two parts. In the first part, we observe the average time spent by the bank and the e-commerce separately for the first registration of the user by the e-commerce company. The average total running time for whole process is 1330 milliseconds where 79.8 milliseconds is spent by the bank for the computations and the rest is mainly for the communication between all the parties including the e-commerce. Note that, about 220 milliseconds are spent for executing SSL which is to secure Transportation Control Protocol (TCP).

In the second part of the test, we observe execution time for latter (2nd and onward) payment processes. The observed average time for the scheme to authenticate the user and to complete a payment is 288.8 milliseconds where almost all computation time is spent by the bank and the rest is for the communication. We note that a bank uses an average 0.1 MB memory for each authentication where we apply a group of size 2048 bits, in other words we consider the group G as the multiplicative group a finite field $\mathbb{F}_p$ where p is a prime of 2048 bits. Fig. 9 (a) and (b) depict the execution time comparisons of the protocols.

As illustrated in Fig. 9 (a) and (b), the running time of the SES scheme is much less when compared to SET and 3D Secure protocols where both manual and automatic user data entrance are considered.

Remark 1: The SSL protocol is an add-on to secure Transportation Control Protocol (TCP) and SSL involves the communication phases of all these three schemes. We conduct tests to observe only SSL burden on the total execution time of each scheme. The average executing time of SSL for a two-party communication is 110 milliseconds. This observation shows that SSL has taken bulk of the time spent on SES algorithm.

VI. CONCLUSION AND FUTURE WORK

In this paper, we present a protocol, SES, which alleviates the security risks of e-commerce cyber systems and provides a secure method for online shoppers. The method requires computational tasks to be performed by the bank and removes the requirement of storing the users' private data in the e-commerce companies' side. SES provides a secure e-commerce protocol which ensures that the user data cannot be revealed without adequate information gathered from all legitimate actors which are the user, the e-commerce company and the bank. In other words, the bank processes a user's information and manipulates it to be sent to e-commerce company. The manipulated version is only used by the bank for confirmation of customers' future online transactions.

In the presented protocol, e-commerce company would be relieved from investing costly measures to assure the security of its stored data. In addition, the customer is required to enter his/her information for only once and the future transactions would not require the customers re-entry of their data. Furthermore, the data in e-commerce company's side cannot be converted to a meaningful message except by the customers' credit card provider which in general is a bank. In this way, users' privacy will be preserved along with the pressure for protecting customers' data on the e-commerce company will be relatively eliminated. We conducted real time tests to compare the performance of SES and other known e-commerce protocols. Even though most of the computational tasks are carried out by the banks, the final execution time of SES is still competitive to other approaches. We also analyzed the proposed method against the well-known attacks. The analysis indicates that the proposed scheme is secure against the well-known replay and man-in-the-middle attacks. This scheme, SES,

relieves the users from re-entering their data in future online shopping. The data stored in an e-commerce company's database is the manipulated version of users' information and it can only be converted to original form by users' bank. Therefore, in case of a bridge or compromise of e-commerce database, the customers' privacy is still protected. In other words, the method eliminates the security risks on the e-commerce companies which eventually release them from high investment costs to secure their system. Even though, our proposed method requires certain computational tasks need to performed especially on bank side, the overall computational cost is less than its competitors as demonstrated by the experimental results. As a future work, the adaption of SES to other online services, like mobile payment, tax/insurance payment etc. will be conducted.

REFERENCES

[1] A. Hern. *Equifax: Credit Firm Was Breached Before Massive May Hack*. Accessed: Jul. 10, 2021. [Online]. Available: https://www.theguardian.com/technology/2017/sep/19/equifax-credit-firm-%march-breach-massive-may-hack-customers

[2] *McAfee Labs Threats Reports*. Accessed: Jul. 10, 2021. [Online]. Available: https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/repor%ts.html

[3] P. Carsten. *Hackers Attack 20 Million Accounts on Alibaba's Taobao Shopping Site*. Accessed: Jul. 11, 2021. [Online]. Available: https://www.reuters.com/article/us-alibaba-cyber/hackers-attack-20-mill%ion-accounts-on-alibabas-taobao-shopping-site-idUSKCN0VD14X

[4] I.-D. Anic, V. Škare, and I. K. Milaković, "The determinants and effects of online privacy concerns in the context of e-commerce," *Electron. Commerce Res. Appl.*, vol. 36, Jul. 2019, Art. no. 100868.

[5] *How Has COVID-19 (Coronovirus) Affected Your Shopping*. Accessed: Jul. 11, 2021. [Online]. Available: https://www.statista.com/statistics/1110822/coronavirus-impact-on-shopp%ing-online-U.K.-consumers/

[6] K. Hickman and T. Elgamal, "The SSL protocol," Internet Draft RFC, Netscape Commun. Corp., Tech. Rep., Jun. 1995.

[7] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing electronic commerce: Reducing the SSL overhead," *IEEE Netw.*, vol. 14, no. 4, pp. 8–16, Jul. 2000.

[8] S. Lu and S. A. Smolka, "Model checking the secure electronic transaction (SET) protocol," in *Proc. MASCOTS 7th Int. Symp. Modeling, Anal. Simulation Comput. Telecommun. Syst.*, Oct. 1999, pp. 358–364.

[9] *EMV 3D Secure*. Accessed: Jul. 13, 2021. [Online]. Available: https://www.emvco.com/emv-technologies/3d-secure/

[10] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2018.

[11] S. Solat, "Security of electronic payment systems: A comprehensive survey," 2017, *arXiv:1701.04556*.

[12] W. Ford and M. S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*. Upper Saddle River, NJ, USA: Prentice-Hall, 1997.

[13] G. J. Udo, "Privacy and security concerns as major barriers for e-commerce: A survey study," *Inf. Manage. Comput. Secur.*, vol. 9, no. 4, pp. 165–174, Oct. 2001.

[14] O. A. Raheem, "E-commerce security: Classifications and arts," in *Proc. Int. Conf. Comput. Appl. (ICCA)*, Aug. 2018, pp. 1–3.

[15] M. L. Barnes, Jr., "System, method, and computer program product for providing location based services and mobile e-commerce," U.S. Patent 7 487 112, Feb. 3, 2009.

[16] R. Chelliah, J. S. Cornez, C. Dellar, S. Harrison, J. A. Hempe, C. C. Hsu, E. J. Golin, C. A. Price, N. S. Rutta, T. A. Wood, and W. K. Yamamoto, "Computer system and method for electronic commerce," U.S. Patent 5 710 887, Jan. 20, 1998.

[17] R.-J. Hwang, S.-H. Shiau, and D.-F. Jan, "A new mobile payment scheme for roaming services," *Electron. Commerce Res. Appl.*, vol. 6, no. 2, pp. 184–191, Jun. 2007.

[18] M. Niranjanamurthy and D. Chahar, "The study of e-commerce security issues and solutions," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 7, pp. 2885–2895, 2013.

[19] P. Syverson, "A taxonomy of replay attacks [cryptographic protocols]," in *Proc. Comput. Secur. Found. Workshop VII*, Jun. 1994, pp. 187–191.

[20] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: Validating SSL certificates in non-browser software," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2012, pp. 38–49.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[22] S. Thomas, *SSL and TLS Essentials*, vol. 3. Hoboken, NJ, USA: Wiley, 2000.

[23] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*, vol. 1. Reading, MA, USA: Addison-Wesley, 2001.

[24] R. Rivest, *The MD5 Message-Digest Algorithm*, document IETF RFC 1321, Tech. Rep., Apr. 1992.

[25] R. Rivest, *The MD5 Message-Digest Algorithm*, document IETF RFC 1321, Tech. Rep., Apr. 1992.

[26] H. K. Lee, T. Malkin, and E. Nahum, "Cryptographic strength of ssl/tls servers: Current and recent practices," in *Proc. 7th ACM SIGCOMM Conf. Internet Meas. (IMC)*, 2007, pp. 83–92.

[27] D. Eastlake and P. Jones, *U.S. Secure Hash Algorithm 1 (SHA1)*, document IETF RFC 3174, Tech. Rep., Sep. 2001.

[28] D. Wagner and B. Schneier, "Analysis of the SSL 3.0 protocol," in *Proc. 2nd USENIX Workshop Electron. Commerce*, vol. 1, no. 1, 1996, pp. 29–40.

[29] C. Meadows and P. Syverson, "A formal specification of requirements for payment transactions in the SET protocol," in *Proc. Int. Conf. Financial Cryptogr.* Berlin, Germany: Springer, 1998, pp. 122–140.

[30] E. A. Morse and V. Raval, "PCI DSS: Payment card industry data security standards in context," *Comput. Law Secur. Rev.*, vol. 24, no. 6, pp. 540–554, Jan. 2008.

[31] S. J. Murdoch and R. Anderson, "Verified by visa and mastercard securecode: Or, how not to design authentication," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2010, pp. 336–342.

[32] *All You Need to Know About Tokenization*. Accessed: Jul. 18, 2021. [Online]. Available: https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenizati%on-infographic.pdf

[33] B. Leiding and A. Norta, "Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance," in *Proc. Int. Conf. Future Data Secur. Eng.* Cham, Switzerland: Springer, 2017, pp. 181–196.

[34] A. Norta, R. Matulevičius, and B. Leiding, "Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns," *Comput. Secur.*, vol. 86, pp. 253–269, Sep. 2019.

[35] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019.

[36] Q. Zagarese, F. A. G. Rodriguez, P. Powlesland, P. Greci, L. Withers, E. S. F. Loughlin-Mchugh, and R. E. Szczesniak, "Secure electronic payment," U.S. Patent 10 692 085, Jun. 23, 2020.

[37] E. J. Hogan, "Method and system for conducting secure payments over a computer network without a pseudo or proxy account number," U.S. Patent 7 177 848, Feb. 13, 2007.

[38] K. L. Ginter, V. H. Shear, F. J. Spahn, D. M. Van Wie, and R. P. Weber, "Trusted infrastructure support system, methods and techniques for secure electronic commerce transaction and rights management," U.S. Patent 6 658 568, Dec. 2, 2003.

[39] M. Wang, Z. Ding, and P. Zhao, "Vulnerability evaluation method for E-commerce transaction systems with unobservable transitions," *IEEE Access*, vol. 8, pp. 101035–101048, 2020.

[40] Z. Wang, W. Luan, Y. Du, and L. Qi, "Composition and application of extended colored logic Petri nets to E-commerce systems," *IEEE Access*, vol. 8, pp. 36386–36397, 2020.

[41] L. Zheng, G. Liu, C. Yan, C. Jiang, and M. Li, "Improved TrAdaBoost and its application to transaction fraud detection," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 5, pp. 1304–1316, Oct. 2020.

[42] R. Al-Jaljouli, J. Abawajy, M. M. Hassan, and A. Alelaiwi, "Secure multi-attribute one-to-many bilateral negotiation framework for E-commerce," *IEEE Trans. Services Comput.*, vol. 11, no. 2, pp. 415–429, Mar. 2018.

[43] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[44] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl. (MARK)*, Jun. 1979, p. 313.
[45] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[46] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.
[47] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.
[48] D. S. Dummit and R. M. Foote, *Abstract Algebra*, vol. 3. Hoboken, NJ, USA: Wiley, 2004.
[49] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[50] J. Daemen and V. Rijmen, "AES proposal: Rijndael," in *Proc. 1st Advanced Encryption Standard (AES) Conf.*, 1998, pp. 1–45.
[51] *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication, Washington, DC, USA, 1977.
[52] *Python Cryptography Toolkit (Pycrypto)*. Accessed: Jul. 24, 2021. [Online]. Available: https://pypi.org/project/pycrypto/
[53] *Stripe for 3D Secure*. Accessed: Jun. 22, 2021. [Online]. Available: https://stripe.com/docs

SENA EFSUN CEBECI (Graduate Student Member, IEEE) received the B.S. degree in computer engineering and computer science from Bahcesehir University, in 2008, and the M.S. degree in computer science from Oakland University, in 2010. She is currently pursuing the Ph.D. degree with the Applied Informatics, Cybersecurity Engineering and Cryptography Program, Istanbul Technical University. Her research interests include cybersecurity, cryptography, elliptic curve cryptography, symmetric encryption, energy efficiency in peer-to-peer networks, and distributed systems.

KUBRA NARI (Graduate Student Member, IEEE) received the B.S. degree in mathematics and computer sciences from Istanbul Kultur University and the M.Sc. degree in cyber security engineering and cryptography from the Informatics Institute, Istanbul Technical University, Turkey, where she is currently pursuing the Ph.D. degree with the Department of Cyber Security Engineering and Cryptography. She is also working as a IT Specialist of the National HPC Center of Turkey (UHeM).

ENVER OZDEMIR (Member, IEEE) received the Ph.D. degree in mathematics from the University of Maryland, College Park, MD, USA, in 2009. He was a member of the Coding Theory and Cryptography Research Group (CCRG), Nanyang Technological University, Singapore, from 2010 to 2014. He is currently an Associate Professor at the Informatics Institute. He is also the Deputy Director of the National HPC Center of Turkey. His research interests include cryptography, computational number theory, and network security.