CHAPTER 3

E-COMMERCE PROTOCOL RESISTANT TO CYBER ATTACKS

Nafiz ÜNLÜ[1]
Mehmet Emre YAĞAR[2]

INTRODUCTION

Dramatic developments in technology have led to a revolutionary transformation both in social life and economy in 2000s. Web technologies have become an integral part of life at an unprecedented pace. Similarly, beginning from the fixed web services and then, even more with the mobile devices, unpredictable growth in the use of web connection has resulted in an exponential growth in the amount of commercial transactions conducted over the internet (Calzada & Tselekounis, 2018). All of this has created a major paradigm shift in society that has affected purchasing habits of users and the ways of companies to sell their products and services (Treiblmaier, Mirkovski, Lowry & Zacharia 2020). As a result, cyber security has evolved in lockstep with the advancement of communication technology. (Etemadi, Van Gelder & Strozzi 2021). Cybersecurity, like the technologies that are constantly emerging in this new digital economy, has taken on new significance in this new context. So-called cybercriminals take use of speed, mobility, data, and information sharing in order to benefit fraudulently (Dupont & Lusthaus) (2021). When it comes to cybersecurity, some of the fraudulent behaviors include data theft, phishing, attempted fraud, and web service blocking (Benz & Chatterjee, 2020). As a result, e-commerce has become one of the most vulnerable sectors when it comes to cyber security threats. As a result, while starting an e-commerce business, it's critical to think about cyber dangers and data security (Girsang, Candiwan, Hendayani & Ganesan 2020). The recent pandemic crisis affecting world economies has forced organizations to redesign their working models by leveraging digital technologies to ensure the continuity of existing operations, albeit remotely (Keenan, 2020). This change has affected most the employees of companies that saw their work habits have radically

[1] Assist. Prof. Dr. İstanbul Technical University, Informatics Institute nafiz.unlu@gmail.com
[2] Msc, İstanbul Technical University, Informatics Institute, yagar17@itu.edu.tr

changed (Huertas-Valdivia, Ferrari, Settembre-Blundo & García-Muiña 2020; Miceli, Hagen, Riccardi, Sotti & Settembre-Blundo 2021), but consumer behavior has also been affected by this, too (Amicarelli, Tricase, Spada & Bux 2021). Individual's habits of choosing and purchasing a product or service online have changed, forcing manufacturers and retailers to adapt their offerings to new demand requirements, particularly by leveraging the widespread use of technology and customer data (Grewal, Gauri, Roggeveen & Sethuraman 2021).

Online shopping or retailing is a form of electronic commerce that allows consumers to buy and sell goods directly over the Internet using a web browser. Commercial activities on Internet have been growing rapidly in the last few years (Greenstein, 2015; Vysotska et al., 2020). When it comes to payment, the sense of security comes to the fore as a need. The customer must be able to choose a payment method, and the software must verify the customer's payment qualification. Maintaining transactions that require a very high degree of trust makes it difficult to flow information over an unreliable public network such as the Internet.

Confidentiality has become a major concern for consumers with the increase of identity theft and impersonation, and this problem experienced by consumers is actually becoming a huge problem for sellers as well (Güllü & Didem, 2018; Marangoz, 2018). Access to and repetition of sensitive information are some of the methods used by hackers in e-commerce (Atakan, 2021). The increase in the volume of electronic commerce compared to recent years and the further development of obtaining personal data become the focal point of those who intend to attack and cause emergence of new methods (Aydin & Derer, 2015). Not only that the customer is unconscious, but also the inadequacy of the applied system helps the attackers to hunt the users easily. Therefore, it shows that security in e-commerce is essential and an important problem (Çinar & Bilge 2016).

Recently released viruses such as Melissa and ILOVEYOU are highly effective in attacks against websites such as Yahoo, Amazon, eBay, and it stands out as a primary security problem for people who do their business over the internet (Boholm, 2021; Knight, 2000).

This study is about presenting methods to e-commerce security protocols at first and then proving the benefits of using encryption methods in e-commerce.

General Model of Security in E-Commerce

E-commerce is a vital component of the internet. Network security is the foundation of e-commerce security. The requirements of e-commerce security (Çetintaş, 2018) can be stated by the following five factors based on the features

of e-commerce.

1. Security: This prevents unauthorized individuals from obtaining information. It's possible with symmetric encryption techniques like Serpent and AES.
2. Integrity: This prevents unauthorized individuals change information. To do this, the Message Authentication Code is used.
3. Accessibility: It is the availability of information without changing it for as long as it is needed. It necessitates a variety of security measures and encompasses numerous areas of data protection. Intrusion detection and prevention, for example, and disaster recovery.
4. Undeniability: This guarantees that neither party can deny the data exchanged between the parties. Digital signature is one method used to ensure this.
5. Suitability: This is to prevent the cases such as unpaid deliveries or undelivered payments. Conformity is closely related to non-denial (Ratnasingham, 1998, Table 1).

Table 1. Attacks on Computer Systems

Attack	Targeted Security Element	Approaches	Solution
Interruption	Availability	Hardware Destruction Physical damage to communication lines Noise Emission Routing deception Script or file deletion DoS attacks	No effective solution
Intercept	Confidentiality and Privacy	Eavesdropping Line Tracing Packet capturing Handshaking Changing database records	Encryption – decryption
Modification	Integrity	Utilizing delays in communication Modifying hardware Adding new record to database	Digital signature for each package of message
Fabrication	Authenticity	Adding new network package by IP-deception Using fake e-mail or region names	Authentication

E-commerce works over the Internet or intranet. B2B and B2C are the major transaction types (Asare, Gopolang & Mogotlhwane 2012). The public key infrastructure (PKI) for identifying or authenticating the other party on the Internet provides the most reliable solution for this necessity. Various security services can be built using PKI. Digital signature and key management are two of the security services available. SSL and SET, which are built on PKI and other cryptographic foundations, are the most essential e-commerce protocols (Akleylek, Yıldırım & Tok 2011). SSL is located between the TCP and application layers. It's used to help secure web browsing. SSL is a solution for transaction authentication, confidentiality, and integrity. SET is an open standard for securing credit card transactions over the Internet. Cryptographic foundations include symmetric key ciphers like those used in SSL and SET. Other protocols exist to address specific e-commerce issues. The topics of unquestionability and suitability are examined, and several protocols or research are suggested. (Turnaoğlu, 2015). New e-commerce protocols are predicted to arise in tandem with e-commerce development, and these protocols are likely to be built on PKI and other cryptographic foundations similar to existing protocols. These e-commerce protocols can be used to create unique e-commerce apps. Distinct security policies and protocols should be defined for different applications. As a result, we provide a general security model for e-commerce. The overall concept can meet e-commerce security needs. Table 1 depicts this model. SSL and SET will be mentioned in this model

General Model of Security in E-Commerce

The two most important protocols currently used in e-commerce are SSL and SET (Zhiguang, Xucheng & Rong 2004). These two protocols sit on top of information security structures like PKI and beneath some e-commerce systems. Today, SSL or SET is used in practically all e-commerce applications. These two protocols will be discussed in greater depth further down.

SSL

SSL is a TCP-based security protocol that provides end-to-end protection. Netscape Communications created this protocol, which has since become an Internet standard known as transport layer security (TLS) (IETF, 1999). The protocol stack for SSL can be seen in Figure 1. There are four subprotocols to the SSL protocol: 1) SSL registration; 2) SSL handshake; 3) Password Attribute Protocol; 4) Alert Protocol.

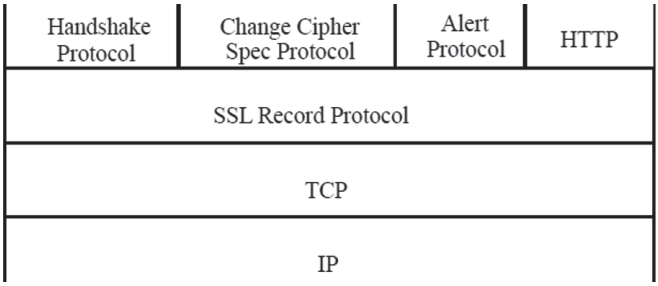

Figure 1. SSL Protocol Stack

The two main sub-protocols are the SSL registration protocol and the handshake protocol. The SSL registration protocol establishes the data transmission format and provides two SSL services:

1. Security: The Handshake Protocol defines a secret key known only to the customer and vendor, which is used for encryption of SSL payloads.
2. Message Integrity: The Handshake Protocol also contains a secret key that is used to generate a message authentication code (MAC).

When establishing an SSL connection, the SSL handshake protocol uses the SSL logging protocol to transmit a sequence of messages between the SSL vendor and the consumer. This message exchange is intended to make the following actions easier: 1) The server verifies the client's identity. 2) Enabling both the client and the server to select cryptographic algorithms or ciphers that they both support. 3) Authenticate the client with the server if desired. 4) Encryption of data in shopping using public key encryption techniques. 5) Setting up a secure SSL connection.

Despite the general acceptance of the SSL architecture, this protocol has some vulnerabilities. The man-in-the-middle attack is the most common SSL attack. SSL allows many key exchange algorithms. However, a man-in-the-middle attack can easily occur if the participants of a session do not authenticate each other. Certified key contract algorithms should be used to prevent it. Another issue is that the present web browser's encryption is insufficient.

Some of the advantages of using the SSL protocol are:

1. SSL is absolutely transparent to vendor's software or customers because it provides security at the session layer. This is especially beneficial for vendors because, aside from the cost of installing certificates, integrating SSL with their existing systems is free.

2. SSL is already built into common Web browsers and there is no need to install any additional software.
3. The SSL system is uncomplicated, resulting in minimal impact on transaction speed.

The SSL protocol has disadvantages as well as its advantages:

1. SSL only secures the connection between the client and the vendor. The seller is allowed to see the payment information. SSL cannot guarantee that the seller will not misuse this information or protect it from intrusion while it is stored on the seller's server.
2. Without a third-party server, SSL cannot guarantee the non-repudiation principle.
3. SSL unnecessarily uses the same strength for all data exchanged although not all data requires the same protection level. To exemplify, an order list does not need a very strong encryption, unlike information that belongs to a bankcard. Using the same key intensity for both results in wasted processing time.

SET General Protocol

The SET protocol was created in 1996 with the joint effort of MasterCard, Visa and other industries. The security problems of SSL/TLS used in e-commerce indicate that new solutions are needed. The purpose of SET is to solve the problem of payment security on the Internet. The SET protocol basically provides four security services (Nada, 2018).

1. *Confidentiality of the message:* The account's message and payment are secure when transported over the network. The number of credit cards is known to the bank, but not to the seller. The SET protocol uses various symmetric encryption algorithms to ensure message confidentiality.
2. *Integrity of data:* Using RSA digital signature and SHA digest function for data such as subscription, personal data, payment method sent to the seller, SET guarantees that the migrated data cannot be changed illegally.
3. *Verifying the cardholder's account:* Merchants can verify that the cardholder is the original owner of the card. SET achieves this using the X.509 digital certificate and the RSA digital signature algorithm.
4. *Seller authentication:* The cardholder can verify the identity of the seller and confirm the business relationship between the seller and the financial institution. Next, the amount of the credit card payment is determined.

There are several advantages of using the SET protocol:

1. SET provides business protection and breakdown of costs incurred, along with adequate security for electronic payment transactions; besides, it prevents credit card fraud (AliShirvani & Mortazavi 2016).
2. SET provides online vendor reliability.
3. SET ensures that confidential information is kept and increases the quality of online shopping. In the SET protocol, the card number of the cardholder is never stolen.
4. SET offers banks and card-issuing financial institutions wider internet access and reduces the risk of online credit card fraud.
5. SET creates common ground at every stage of its online process; Thus, it is ensured that a system is established on the products of different enterprises.

In addition to the advantages of the SET protocol, it has some disadvantages and limitations, too:

1. SET does not guarantee that it will transfer goods marketed to the buyer after payment has been made through the gateway.
2. SET does not offer any method to guarantee the quality of purchased products; if the products are not as customers demand, they should be able to exchange or withdraw the fee paid (Ren, Wei, Zhang & Ma 2011).
3. SET does not guarantee end-to-end security (customer to vendor). A network can be attacked by any organization at any time during the transaction process; If a network is hacked, money can be taken from customers' accounts without their knowledge.
4. SET does not guarantee end-to-end security (customer to vendor). A network can be attacked by any organization at any time during the transaction process; In the event of a network hacking, money can be withdrawn from customers' accounts without their knowledge (Sanyal, Tiwari & Sanyal 2010).
5. SET is practically quite large and complex. During the typical SET process, it needs to perform 9 confirmations, 7 data transfers with a digital certificate; digital signature requires 6 confirmations, 5 signatures, 4 symmetric encryption and 4 asymmetric encryption. The SET protocol includes many entities such as customers, marketers and the financial industry. In order for them to work together, they need to change their systems. During the SET protocol, customers must have a banking application installed on their computers and use certificates in all transactions. Therefore, the SET is relatively costly to implement (Boping & Shiyu 2009).

The interaction between business entities in the SET (Saqib et al., 2019) is illustrated in Figure 3. A typical purchasing process is shown below:

1. The customer creates a bank account.
2. The customer obtains an electronic certificate that can be used to complete an online transaction.
3. The certificates are delivered to the seller. Two certificates for the vendor's two public keys are required. The communication is signed with one public key, while the other is used for key exchange. For the point of payment, the seller additionally need a copy of his certificate.
4. The customer makes a purchase. The buyer verifies seller over the browser. Order and payment information are sent over the browser. Public keys of seller and bank are used to encrypt order and payment information, respectively.
5. The seller requests payment sanction. This transaction ensures that the customer has enough funds to make this payment.
6. The seller confirms this order and sends this information to the customer.
7. The seller offers the goods or services.
8. The seller requests payment from the bank.

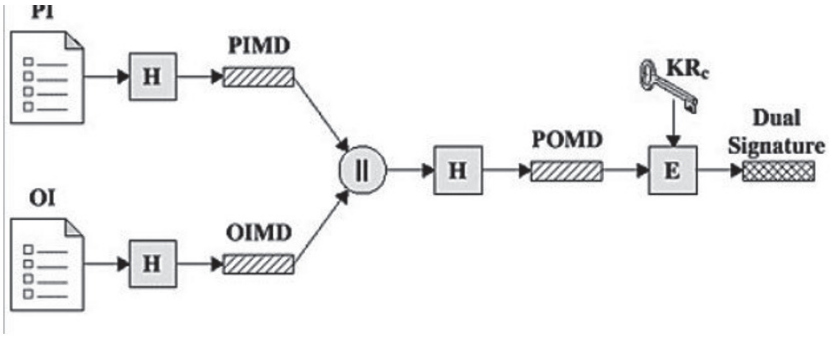

Figure 3. Dual Signing (Saqib et al., 2019)

Implementation of the SET

In the SET protocol, the identity of both the seller and the cardholder is protected, and the cardholder knows that the transaction he has made after the purchase is based on the principle of non-repudiation. The most important factor in this protocol is that the customer signs separately for both the seller and the payment point (bank).

After the customer first takes the hash values of the payment information and the order information separately and combines them, he signs the hash value of the obtained data with the customer's private key and obtains the binary signature format.

The customer prepares the following package for the bank. First, it determines a key value and encrypts this key with the bank's public key. Payment information, binary signature and hash value of order information are encrypted with the key specified by the customer. Using this encrypted value and the bank's public key, the encrypted key is sent to the bank. The striking point here is that the bank does not know how the customer placed an order, because the customer sends the summary value of the order information to the bank, which shows that the confidentiality element is provided (Stallings, 2002).

The customer also prepares the following package for the seller. Order information, binary signature and hash value of payment information are sent to the seller. At this point, the seller should not access this bank account information, so the summary value of the payment information is sent to the seller.

The bank and the vendor process the packages they receive in the same way and verify the binary signature on the package. The order process is completed with the verification of the double signature.

3-D Security Protocol

Credit card and online payment transactions have become a part of daily life. Many people use credit cards from Visa or Mastercard companies. These companies produce solutions for credit cards and other payment systems for banks. What does 3D Security mean in this case? 3D Security is an XML-based protocol used as a security layer for online credit or debit card transactions. The purpose of this protocol developed by Visa company is to increase the security level of internet payments. In general, 3D security is mentioned as popular operations today. It is used in all credit card and internet payment transactions. The aim is to create a more secure protocol for the transactions performed and to avoid fraud. The basic concept of the protocol is to connect online authentication and financial status.

The protocol uses XML messages sent over SSL connections with Client Authentication (this ensures the authenticity of both Peers, Server and Client using Digital Certificates) (Koç, 1999).

3D security is specified as a security protocol used to authenticate users. This creates an extra layer of protection for payment card transactions in the scenario where the card cannot be used. It is designed to allow a cardholder to authenticate when making a payment to prevent inappropriate or unauthorized transactions and reduce rejections.

The purpose of 3DS authentication is to verify the identity of the cardholder and establish the financial authorization process. The model works with the following three-step method:

1. Buyer domain – environment of the receiving bank and the merchant receiving the payment
2. Issuer domain – environment of the issuing bank that issues the card
3. Interoperability space – existing system that supports the 3-D security process by allowing the parties in the transaction to interact and exchange information

3DS authentication uses the Secure Sockets Layer (SSL) protocol to send Extensible Markup Language (XML) messages with client authentication. Digital certificates are used to verify the identity of all parties during the transaction. Thus, maximum security is ensured with this process.

Introduced in 2015, this protocol provides a less intrusive authentication process to reduce redundant transactions in 3DS transactions (when users are redirected to the card issuer's website to verify transactions). With 3D security version 2.0, marketers are now required to submit authentication data along with payment card information to verify the authenticity of the transaction. Thus, it happens invisibly to the user and the identity of the payment is revealed if the payer finds a reason for the legitimacy of the transaction. If suspicious behavior or transaction from an unknown device is detected, the user will now receive a text message or confirmation code via an app instead of being redirected to a bank's website to verify their identity. The result will be a much less distracting application experience for the user (VISA, October).

3-D security provides a global framework with authentication for remote payments. It reduces the expenses during the process by making a refund after the unauthorized person's transaction.

Besides advantages of 3-D security, it also includes some disadvantages. The user may find it difficult to distinguish between the real payment page and the fake payment page, which brings with it phishing. Cardholders, who do not want to risk having their card stolen while shopping on another trading site, can enter their bank's home page from a separate window and register here. When they return to the trading site and start over, they should see that their card is registered. The presence of the Personal Assurance Message (KGM) they chose while signing up on the password page is confirmation that the page came from the bank. It still shows the possibility of a man-in-the-middle attack if the cardholder fails to verify the SSL Server Certificate for the password page.

3D security and most of the security requirements are handled by TLS/SSL. It is more secure than the SET protocol. Responsibility for fraud now rests with the cardholder, not the card company. It is an extensible global development that ensures the confidentiality of information, payment integrity and authenticates cardholders.

Privacy and E-Commerce

When a customer signs up for an e-commerce site, the information they enter may not be authentic so it is not known whether they are really interested in purchasing. For example, cash-on-delivery purchases with a fake phone number and address can result in huge revenue losses. That's why it's important to authenticate online for every potential customer.

The information of customers who authenticate online is stored in the database. In the event of any attack, this information can fall into the hands of malicious people. This scenario is one of the problems in the e-commerce business that should not be ignored and is definitely one of the worst nightmares of every e-commerce owner.

It should protect the personal data of e-commerce site visitors and customers and have data privacy measures.

The precaution that can be taken individually is to check whether the site fulfills the requirements of the KVKK No. 6698 before sharing personal data, to examine the clarification texts in detail, and to investigate whether there are personal data protection policies.

Future Planned Works

The disadvantages of the SET protocol are mentioned above. Draft designs to correct these disadvantages can be made and then put into practice. One way to overcome the limitations of the SET protocol is to use the electronic transaction authentication system, which can be replaced by the certificate authority.

Security and trust are the two most important factors in the e-commerce concept. In the token-based SET protocol, considerations of trust, customer satisfaction, and end-to-end security between merchants and customers are taken into account. This protocol has a trusted third party that uses the SLL protocol. Logs of all transactions are kept and this log information will be used in case of any dispute with the presence of a trusted third party. Recorded transaction logs will get real records of all transactions performed and will have resolved any issues such as possible delay or non-payment of debt amount. In addition to all these, data is

recorded to ensure the reliability of workplaces. Customers will be able to access these recorded data before taking any action.

REFERENCES

Akleylek, S., Yıldırım, H. M., & Tok, Z. Y. (2011). Kriptoloji ve uygulama alanları: açık anahtar altyapısı ve kayıtlı elektronik posta. *Akademik Bilişim*, 713-718.

AliShirvani, N., & Mortazavi, B. (2016). Guaranteeing of trust and security in e-commerce by means of improved set protocol. *Bulletin De La Société Royale Des Sciences De Liège*, 1136-1147.

Amicarelli, V., Tricase, C., Spada, A., & Bux, C. (2021). Households' food waste behavior at local scale: a cluster analysis after the COVID-19 lockdown. *Sustainability*, *13*(6), 3283.

Asare, S. D., Gopolang, B., & Mogotlhwane, O. (2012). Challenges facing SMEs in the adoption of ICT in B2B and B2C E-commerce: A comparative case study of Botswana and Ghana. *International Journal of Commerce and Management*, *29(4)*, 272-285.

Atakan, M. (2021). Siber Güvenlik ve Covid 19 Salginin Uzaktan Denetim Üzerinde Etkileri. *Denetişim*, *(22)*, 27-39.

Aydin, S., & Derer, E. (2015). E-Ticarette Güven Unsurunun Müşterilerin Satin Alma Davranişlarina Olan Etkisi: Süleyman Demirel Üniversitesi Öğrencileri Üzerine Bir Araştirma. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *(21)*, 127-150.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63(4)*, 531-540.

Boholm, M. (2021). Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019). *Journal of Cybersecurity*, *7(1)*, 1-23.

Boping, Z. & Shiyu, S. (2009). An Improved SET Protocol. In F. Yu, J. Shu & G. Yue (Eds), *Proceedings of the 2009 International Symposium on Information Processing (ISIP'09)*, (pp. 267-272).

Calzada, J.; Tselekounis, M. (2018). Net Neutrality in a hyperlinked Internet economy. *International Journal of Industrial Organization,* 59, 190-221.

Çetintaş, E. (2018). *Sosyal medya ve e-ticaret kullanıcılarının gizlilik ve güven algılarının değerlendirilmesi: Türkiye-ABD karşılaştırması* (Unpublished master›s thesis). Yalova University, Yalova.

Çinar, I., & Bilge, H. Ş. (2016). Web Madenciliği Yöntemleri ile Web Loglarının İstatistiksel Analizi ve Saldırı Tespiti. *Bilişim Teknolojileri Dergisi*, *9*(2), 125.

Dupont, B., & Lusthaus, J. (2021). Countering distrust in illicit online networks: The dispute resolution strategies of cybercriminals. *Social Science Computer Review.* doi: 0894439321994623.

Etemadi, N., Van Gelder, P., & Strozzi, F. (2021). An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity. *Sustainability*, *13*(9), 4672.

Girsang, M.J.; Candiwan; Hendayani, R.; Ganesan, Y. (2020). *Can information security, privacy and satisfaction influence the e-commerce consumer trust*? In 2020 8th International Conference on Information and Communication Technology (ICoICT) doi: 10.1109/ICoICT49345.2020.9166247.

Greenstein, S. (2015). *How the internet became commercial.* Princeton: Princeton University Press.

Grewal, D., Gauri, D. K., Roggeveen, A. L., & Sethuraman, R. (2021). Strategizing retailing in the new technology era. *Journal of Retailing*, *97*(1), 6-12.

Güllü, K., & Didem, A. (2018). Tüketicilerin Seyahat Acentaları Web Tabanlı Uygulamalarını Etik Yönden Değerlendirmeleri. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 9(16), 1254-1284.

Huertas-Valdivia, I., Ferrari, A. M., Settembre-Blundo, D., & García-Muiña, F. E. (2020). Social life-cycle assessment: A review by bibliometric analysis. *Sustainability*, *12*(15), 6211.

IETF. The TLS Protocol Version 1.0[EB/OL]. Retrieved from http://www.ietf.org/rfc/rfc2246.txt, 1999-01-05

Keenan, J. M. (2020). COVID, resilience, and the built environment. *Environment Systems and De-*

cisions, *40*(2), 216-221.

Knight, P. (2000). ILOVEYOU: Viruses, paranoia, and the environment of risk. *The Sociological Review*, *48*(2_suppl), 17-30.

Koç, C. K. (1999). Next Generation E-Commerce Security. *Information Security Laboratory December*, *2*. Retrieved from https://www.just.edu.jo/~tawalbeh/nyit/csci860/notes/nextg.pdf

Marangoz, M. (2018). Tüketici mahremiyetinin korunmasi: sorumlular ve yöntemler üzerine nitel bir araştirma. *Journal of Academic Researches and Studies*, *10*(19), 474-488.

Miceli, A., Hagen, B., Riccardi, M. P., Sotti, F., & Settembre-Blundo, D. (2021). Thriving, not just surviving in changing times: How sustainability, agility and digitalization intertwine with organizational resilience. *Sustainability*, *13*(4), 2052.

Nada M.A.A. (2008). E-Commerce Security. *IJCSNS International Journal of Computer Science and Network Security*, 8(5), 340-344.

Ratnasingham, P. (1998). Trust in web based electronic commerce security. *Information Management & computer security*, *6(4)*, 162-166.

Ren, X., Wei, L., Zhang, J. & Ma, X. (2011). The Improvement of SET Protocol based on Security Mobile Payment. *Journal of Convergence Information Technology*, 6(7), 22-28.

Saqib, M. N., Kiani, J., Shahzad, B., Anjum, A., & Ahmad, N. (2019). Anonymous and formally verified dual signature based online e-voting protocol. *Cluster Computing*, *22*(1), 1703-1716

Sanyal, S., Tiwari, A. & Sanyal, S. (2010). A multifactor secure authentication system for wireless payment. In R. Chbeir, Y. Badr, A. Abraham, & A.-E. Hassanien (Eds), *Emergent web intelligence: Advanced information retrieval* (pp. 341-369). London: Springer.

Stallings, B. (2002). Globalization and liberalization: The impact on developing countries. In States, markets, and just growth: Development in the 21st century, ed. Atul Kohli, Chung-In Moon, and George Sorensen. Tokyo: United Nations Press

Treiblmaier, H., Mirkovski, K., Lowry, P. B., & Zacharia, Z. G. (2020). The physical internet as a new supply chain paradigm: a systematic literature review and a comprehensive framework. *The International Journal of Logistics Management,* 31, 239-287.

Turnaoğlu, M. (2015). *İletişim teknolojisindeki gelişmelerin ticari ilişkilere etkileri ve yeni Türk Ticaret Kanununa yansıması* (Unpublished master›s thesis). İstanbul Ticaret University, İstanbul.

Visa 3-D Secure 2.0 (2022). What is Visa's 3-D Secure 2.0 and how does it work? Retrieved from https://usa.visa.com/visa-everywhere/security/future-of-digital-payment-security.html

Vysotska, V., Bublyk, M., Vysotsky, A., Berko, A., Chyrun, L., & Doroshkevych, K. (2020, September). Methods and tools for web resources processing in e-commercial content systems. In *2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT)* (Vol. 1, pp. 114-118). IEEE.

Zhiguang, Q. I. N., Xucheng, L. U. O., & Rong, G. A. O. (2004). A survey of E-commerce Security. *Journal of Electronic Science and Technology*, *2(3)*, 173-176.