
Mostafa A. Ali², Nazimah Hussinᵇ, Ibtihal A. Abedᶜ, Azman Hashim
International Business School, University Technology Malaysia, Kuala Lumpur, Malaysia, Email: mostafa1988@graduate.utm.my, nazimah@ibs.utm.my, ahmed-1988@graduate.utm.my

In this paper, the major aim is to investigate the heightened awareness regarding various electronic payment systems-related concepts in terms of their advantages, problems, and security issues. The payment processing system providers use software as a service (SaaS) model and with this model, they form a single payment channel to numerous payment methods for their clients. Users often give away their personal information such as names, card details, and so on whenever they go online to make any firm of payment. An online payment system is referred to a system that facilitates electronic money exchange. This form of payment typically involves the deployment of the Internet, computer networks, and other digital stored value systems. Collecting any form of payment over the internet implies that the user has accepted an online payment and must have shared some confidential information with the service provider. This paper embarks on a thorough review of all aspects of online/electronic payment with emphasis on the analysis of numerous studies on electronic payment systems. The latest studies have been explored to gain insight on the electronic payments systems.

Key words: Electronic payment, Information hiding, Steganography, Cryptography.
Introduction

The exchange of goods and services between 2 persons started before the advent of written history; but as the exchange of goods has become more difficult between persons, they began to represented values in an abstract manner, starting with the barter system to the use of certified notes, payment orders, cards (debit or credit), and recently the electronic or e-payment systems (Masihuddin et al., 2019). The customary payment methods are well-known to have certain issues such as false signatures, cash falsification, and bounced cheques. However, a well-planned e-payment system can address these security issues and provide an added advantage of usage pliability (Sun et al., 2011; Aigbe and Akpojaro, 2014). E-payment systems have received much recommendation due to their ease of money exchange, security, and faster access to capital resources (Ayo and Adewoye, 2010; Oyewole et al., 2013; Oyewole et al., 2013). The conventional cash payment systems have become more expensive compared to the recent strategies due to the recent impacts gained by minor financial transactions in most economies. Furthermore, interne cash processing can have less value compared to the smallest cash estimation in the manual world (Singh et al., 2012).

As the web keeps impacting our daily lives, people are getting used to online transactions when buying or selling products (Sharma, 2013). However, the increased dependence on web-based transactions for cash-related activities has come with issues that cannot viably be solved by the traditional payment methods. For this reason, financial experts have begun to investigate different e-payment systems with emphasis on the issues associated with digitalized and e-payment systems (Aigbe and Akpojaro, 2014). Each online transaction is processed through payment gateways which serve as a point for accessing different financial organizations. The payment details between different parties and financial institutions are validated through these payment gateways (Sharma, 2013). In this paper, a detailed description of the increased awareness on electronic payment systems (EPS) was provided. This paper is arranged as follows: section 2 provides various definitions and aspects of EPS while section 3 and section 4 cover the advantages and popularity of EPS. In section (Oyewole et al., 2013) the problems associated with payment system is provided while the important security issues of EPS are presented in section (Singh et al., 2012). A review of the related works to EPS is presented in section (Sharma, 2013) while section 8 concludes the paper.

Electronic Payment System (EPS)

With the increase in the exchange of goods among different business partners over the Internet, the conventional cash-based payment system has been gradually relegated
(Abrazhevich, 2004) as most people prefer an electronic payment system to the cash-based method. These e-payment systems are considered as a method of making payments for services over the Internet (Roy and Sinha, 2014; Kabir, 2015). An EPS can be described as a form of inter-organizational information system (IOS) dedicated for making money-related transactions between customers and different organizations. There may be a need for complex interactions between technologies, the environment, and the partners to ensure an effective EPS. The specific features of EPS/IOS also makes it technologically, organizationally, and relationally different from the traditional internal-based information systems (Ahituv, 1989; Boonstra and De Vries, 2005; Kumar and Crook, 1999). This highlights the need for the cooperation among different technologies to make an effective system (Vu and Proctor, 2011).

Over the years, there has been an increase in the global annual non-cash transactions facilitated through mobile and e-payment systems except for the year 2012 when there was a decline in the annual growth rate from 8.6% in 2011 to 7.7% in 2012 (Mashiuddin et al., 2017). However, the year 2014 witnessed an increase in the global electronic payment to 8.9%, reaching 387.3 billion, representing the most significant increase since the World Payments Report was first published. This increase was mainly due to the quickened development in newly emerging financial markets. A projected higher worldwide development of 10.1% was anticipated for the year 2015 and predicted to take the global non-paper exchange volume to 426,300,000,000 (Mashiuddin et al., 2017). Individuals and groups use e-payment systems as a convenient and secure way of making cash payments over the internet and consider the channel as the gateway to technological advancement in global economy (Slozko and Pelo, 2015). It has also become the major facilitator of e-commerce on which success in electronic business depends upon. E-payment systems have also reduced resourcefulness ad fraud rate in the global payment system (Kabir et al., 2015; Mashiuddin et al., 2015).

**History of EPSs**

Historically, e-payment dates to 1918 when the United States (U.S.) Federal Reserve Bank first moved currency via telegraph. However, this technology was not widely adopted in the US until the incorporation of their Automated Clearing House (ACH) in 1972. Since then, the popularity of the system became high, enabling the U.S. commercial banks and its central treasury to introduce it as an alternative to the conventional cheques payment (Kabir et al., 2015).

The advent of credit cards also date to 1914 when customers were issued with cards by department stores, oil companies, Western Union and hotels to facilitate payment for goods
and services. Forty years later, credit cards are being widely used and have become more acceptable as a payment option. Before the 1990s, credit cards were issued as paper-based payment options but later, they were transformed to electronic systems. The increase in the rate of credit card usage has led to a rapid growth in the industry and has ushered in the introduction of a debit card system. Both credit and debit cards are currently used globally for the payment for goods and services (Roy and Sinha, 2014; Al-Laham, 2009).

**Definitions of EPS**

The EPS is a complex term that portrays various methods of electronic payment delivery. Its multipurpose nature provides and increased imprecision of e-payment characterization in the literature. In terms of capabilities, e-payment can be considered as e-banking, e-cash, internet banking, m-payment, online banking, and so on. All things considered, researchers have recently strived to provide a comprehensive definition of e-payment (Oyewole et al., 2013). The EPS is described by (Abrazhevich, 2004) as a form of financial commitment which brought a customer and a seller to the same platform via electronic means. Furthermore, (Vu and Proctor, 2011) considered e-payment as a form of inter-relation between people and associations powered by institutions that provides electronic financial transactions.

According to (Mieseigha and Ogbodo, 2013), e-payment is any form of internet-based money exchange. Similarly, (Adeoti and Osotimehin, 2012) stated that an e-payment system is an electronic way of making payments for web-based services. In another explanation, e-payment is any form of payments/exchange made electronically (Kabir et al., 2015). Another researcher (Kalakota and Whinston, 1997) considered e-payment as an online monetary exchange between two persons. Additionally, (Masihuddin et al., 2017) defined e-payment as money-related exchanges facilitated via electronic means. Another definition of e-payment is any form of payment that involves exchange of electronic information such as credit and debit card detail other than payment with cash or cheque (Masihuddin et al., 2017).

As per (Antwi et al., 2015), e-payment is a fiscal claim exchange by a payer on a worthy and useful party. According to (Lin and Nguyen, 2011) e-payment involves payments made through electronic transfers, an automated clearing house, or through a commercial card system. E-payment was defined by (Shon and Swatman, 1998) as any form of money exchange via any electronic channel. Another definition of e-payment according to (Gans and Scheelings, 1999) is payments made through electronic signals linked to credit or debit bank accounts. E-payment, as per (Turban et al., 2017) is any form of non-money payment with the exception of a paper cheque. E-payment is defined by (Ming-Yen et al., 2013) as any electronic exchange that could be considered as a form of payment for goods and services.
made via e-payment channels that gives clients a remote access to their financial accounts via electronic systems. Generally, EPS can be defined as any form of monetary exchange between buyers and sellers via online platforms with the help of a digital financial instrument (Oh, 2006).

**Types of E-payment systems**

Several types of EPS have been developed within the global financial system, such as electronic cheques, electronic fund transfers, e-cash, credit and debit card (Kabir et al., 2015; Peffers and Ma, 2003). Online payment can generally be classified into two types; i) based on the Internet Banking Payment Gateway (IBPG) involved, and ii) based on the external payment platform. In the first type, it is a sort of a direct payment as the client is aware of the online payment via an e-business platform which is linked to a banking platform. For the second type, it involves the transfer of fund from the purchaser’s account to the seller’s account by an external payment system. The IBPG connects a banking process system with the Internet; it is specifically designed for the management and authorization of payment. It links the purchaser with the seller and the bank. The IBPG-based online payment method cannot be realized without the involvement of payment gateways (Yang et al., 2007).

A study by (Yu et al., 2002) classified EPSs into four groups that deserves mentioning; these groups are electronic cash, small payments, online credit card payment, and electronic cheques. The study further highlighted that each of these systems is associated with specific advantages and drawbacks. They stated that each of these groups can be assessed from their technological, economic, social and institutional/law aspects. In reality, only two specific kinds are payment systems exist (Aigbe and Akpojaro, 2014; Conrad et al., 2018):

**Based on electronic transaction**

There are four modes of internet-based payment systems:

**Cyber cash**

This is an online service in which a client’s credit card information is processed, charged, and deposited in the dealer’s account via electronic means. In this form of cash transfer, the cyber cash serves act as the payment gateway through which the payment is made. The system depends on digital signatures to ensure the security of the payment process (Conrad et al., 2018). Although e-money is a more extensive concept that involves all internet-based fund transfer, cyber cash mainly emphasizes on all systems of cash exchange processed through the Internet. A clear distinction between e-money and cyber cash may be difficult to establish
since cash money is derived from e-money and is progressively converging into it (Guttmann, 2002).

**Secure electronic transaction (SET)**

This secure electronic money transfer system is an online payment system that guarantees a secure internet-based money exchange. It was created by Master Card and VISA as an open technical platform for business (Lu and Smolka, 1999). SET ensures a secure card-based fund transfer over the Internet. It uses digital certificates to confirm the legitimacy of a vendor or a cardholder (Conrad et al., 2018).

**First virtual holdings**

This is one of the early Internet-based payment platforms that depend on external confirmation techniques to facilitate online payments. This payment system is of particular interest because it does not depend on any form of encryption. It is only used for the selling of data over the Internet, as against the exchange of goods and services. This system uses an automated telephone system to gather the payment information of the participants. Being that it does not depend on cryptographic techniques and digital signatures, it mainly depends on a careful monitoring of sales and purchases to reduce fraud (Masihuddin et al., 2017). As an open system, a principal aspect of this payment system is that some data are not meant to go online since they are essentially related to the financial information of the clients. This system uses a first virtual PIN issued by a first virtual organization for exchange purposes instead of using credit card numbers. Being that these PIN numbers serve as ID, they can be transmitted over the Internet without charging the client’s account since an affirmation email must be received from the client to approve any form of payment (Conrad et al., 2018).

The use of cards as a mode of payment has seen tremendous growth since the year 2010; this is evidenced in the decline in cheque-based transactions in the last 13 years. Debit cards accounts for the highest share among the card-based system as almost 45.7% of the global non-cash money transactions are through debit cards, presenting it as the fastest growing (12.8%) payment option in the year 2014. These figures allude to the better security and convenience of the card-based system compared to other payment options (Masihuddin et al., 2017).

Electronic payments can also be made via mobile platforms; various Android-powered smartphones can provide online payment platforms. Regarding EPS, these mobile applications can
also work well on Desktop computers. Clients can also utilize mobile phones in various platforms to facilitate financial transactions. With the use of mobile internet, clients can transmit PIN numbers or use WAP to make electronic payments over the internet. For E-payment, the debit or credit card transaction performed by a client can be authenticated by a vendor by attaching a device to their mobile phones. In the U.S, a conglomerate of late publicized Power Swipe, which is physically connected to a Nextel telephone, weighing 3.1 ounces, and comprised of a reader for magnetic stripe, goes through a connector for charging the battery of the handset and an infrared port for printing (Masihuddin et al., 2017).

Net bill

This is a payment system that depends on the Internet to facilitate online secure transactions. As a micro-payment system, its server maintains buyers and sellers accounts, enabling clients to make payments for products. Information exchange in this system involves exchange of bits with the customers and could be performed in any internal structure such as the search results of a database inquiry, a page of text, or a software program. Customers are billed based on the number of items they use; unlimited access can also be provided to members (Sirbu and Tygar, 1995). A software with financial tools checks the receipts of the products. In so doing, net bill electronic payment system facilitates the communication between the money tool in the software and the dealers’ server (Conrad et al., 2018).

Internet-Based Payment System

There are four basic methods of Internet-based payment systems:

Debit card

The debit card is the most utilized e-payment platform; its technique combines the concept of Internet banking with Automatic Teller Machine (ATM) card (Kim et al., 2010). With the debit card, holders make a direct payment for goods through the bank. Debit cards gives holders the opportunity to save money in their bank accounts for later withdrawal at the point of sales. Ideally, there are two types of debit cards; these are online and offline debit cards (Conrad et al., 2018).

Smart card

A smart card is a plastic card equipped with microchip on which funds can be pre-loaded and later used to make instant payments. The smart card is also called a chip card (Masihuddin et
al., 2017). The business data of an individual can be stored on smart cards just as a chip card can be used to store cash. The smart card is usually authorized with a PIN which the service provider gives to the user. These cards store data in an encoded form to ensure information security; they have a high processing speed. Examples of smart cards include VISA and Mondex cash cards (Masihuddin et al., 2017).

**Credit card**

This is other form of EPS where cards are issued to the clients by the monetary organization for making online payments (Masihuddin et al., 2017). Credit card is the most commonly used e-payment system. Compared to the other e-payment systems, credit card is not proper to be used for the payment of small values (Kim et al., 2010).

**E-cash**

E-cash was introduced as an alternative to credit cards for online purchases (Kim et al., 2010). It is an electronic payment system where certain cash measures are kept away from the customer’s gadget and made open for online transactions. E-cash can also be described as cash in digital form; it uses a pre-installed e-cash software on the client’s PC to facilitate transactions (Masihuddin et al., 2017). A major attribute of e-cash is its low cost which endears it to clients for small-scale transactions (Kim et al., 2010; Singh and Awasthi, 2013).

**Advantages of EPS**

A review conducted by the Federal Reserve Financial Services Policy Committee for the first time showed that in the U.S, electronic payment exchanges have exceeded cheques payments. The total number of electronic exchanges in the U.S in 2003 was equivalent to USD 44.5 billion, while an equivalent of USD 36.7 billion was recorded in cheque payments (Masihuddin et al., 2017). Evidently, there is a recognizable pattern among buyers; purchasers are noted to be willing to transact electronically via an automated medium while doing their transactions.

The review conducted by (Masihuddin et al., 2017) indicates that the advent of the web has set e-payments on an exponential rate of development. Customers can easily purchase goods on the Internet and send an unencrypted credit card information over the system. This raises the susceptibility of the transactions to frauds. However, the advent of e-payment systems has introduced several secure payment systems, making customers to be more concerned about the security of their personal details. As per (Masihuddin et al., 2017), there are remarkable
financial benefits of e-payments in addition to their security and ease of operation. An expansion of these advantages can contribute immensely to the financial improvement of a country.

The introduction of computerized e-payments helps to develop bank deposits which in this manner, has increased accessibility to business credits (a major driver of financial achievement). The security and advantages e-payments confers them full scale financial advantages (Masihuddin et al., 2017). The influence of introducing e-payments is likened to using the gears on a bicycle. The introduction of an efficient e-payment system into an economy will move the performance of the economy to a greater level. The addition of a well-controlled business and consumer credit will improve the rate of economic development even further.

EPS can help in unmasking shadow economies and bring out hidden exchanges into the banking system; this will bring uprightness, confidence, and cooperation into the economic system. Additionally, (Masihuddin et al., 2017) specified that a relationship exists between the increase in demand deposits and the increase in the volume of point of sales. In the banking sector, automated e-payments serve as a gateway and as a powerful driver for growth. Such payments mop cash from the circulation and into bank accounts, providing low cost funds that can support the banks’ investment lending. With this process, there is a greater accountability and transparency, leading to a better economic performance and a greater efficiency.

Comparatively, e-payment is more beneficial to the buyer (Turban et al., 2017) because most times, a buyer is required to provide his account information such as the card number and the delivering address only once. The information provided by the client is saved in the database of the retailer’s server. On his next visit to the page, the client will only be required to sign in with a personalized username and password. A transaction can simply be completed by simply clicking a mouse as the client only has to only confirm the purchase.

Furthermore, e-payments are believed to cut down organizational expenses (Turban et al., 2017) as the cash spent on paper and postage is saved. Organizations can also enhance client’s preservation via an e-payment system. Customers are more likely to return to an e-commerce platform where their information is already saved.

As per (Masihuddin et al., 2017) e-payments can reduce the cost of transactions and facilitate higher consumption and GDP, boost financial transparency, and increase government efficiency. Furthermore, governments have a significant role to play in creating an ideal
environment for these benefits can be consistently achieved through their economic development plans (Masihuddin et al., 2017).

Similarly, (Humphrey et al., 2001) stated that the use of e-payment systems can ensure several advantages to both clients and sellers due to the reduction in costs, higher security, ease of use, and reliability. A noteworthy advantage is that EPS empowers bank customers to resolve their daily money related-issues without going to the bank, thereby, saving time and cost of handling financial transactions (Appiah and Agyemang, 2004).

As stated by (Humphrey et al., 2000) the cost of a country’s payment system can account for about 3% of its GDP. Being that most e-payment systems cost about 33% to 50% of the paper-based non-money payment, e-payments can clearly reduce the social cost of a payment platform if computerized (Appiah and Agyemang, 2004). Paper-based mistakes and expenses can be reduced via mechanizing and reshuffling e-payments via self-serve channels such as point-of-sale (POS) and ATM systems.

A survey by the Visa Canada Association in collaboration with the Global Insight discovered that e-payment systems confers transaction proficiency to purchasers, banks and the economy. Since 1983, e-payments have contributed about $C 107 billion to the Canadian treasury, and accounts for about 25% of the $C 437 billion accumulated in the Canadian economy over the said period. About $C 60 billion of the increment in Personal Consumption Expenditures was accruable from e-payments over the same period, with credit card contributing a major sum ($C 49.4 billion) compared to debit cards ($C 10.4 billion) (Kumaga, 2011).

The Commonly Used E-Payment Systems

In the world today, the major impact of the Internet is the ability to move businesses from place to place over a website. This is why people can easily buy items from the Internet via several payment gateways. Payment service provider are organizations that facilitates marketing-related online services; they regulate electronic payments by monitoring financial exchanges between sellers and buyers (Masihuuddin et al., 2017). Some of the common payment methods are bank transfers, credit card, and real-time orders. Among the popular online payments systems are Braintree, Stripe, Authorize.Net, PayPal, Dwolla, 2CheckOut, Worldpay, Samurai, Eway, Feefighters, American Express Serve, Icepay, Intuit GoPayment, Amazon Payments, Skrill (previously Moneybookers), V.me by Visa, WePay, Google Wallet Checkout, Square, etc. (Niranjanamurthy, 2014).
Problems of E-Payment Systems

Despite the advantages of EPSs, they are still prone to several challenges in today’s world. The identified problems associated with EPS according to previous studies grouped into infrastructure-related, regulatory related, legal-related, and socio-cultural-related issues (Masihuddin et al., 2017).

Infrastructure-related issues

For an effective deployment of any e-payment system, infrastructure is critical. The establishment of appropriate infrastructure for e-payments is a problem (Taddesse and Kidan, 2005) to have a successful e-payment system, there is a need to ensure a strong financial and infrastructural backing. Several areas in most of the developing nations have no banks or access to the basic infrastructure that drives e-payments. As such, a study by (Khidzir et al., 2018) revealed that Nepalese have no access to electricity and telecommunication and it is not possible to implement an e-payment system.

Regulatory and Legal-related Issues

An effective implementation of e-payments requires the existence of national, provincial or global laws and standards. Most of these components have guidelines on tax evasion, monitoring of e-money institutions, and commercial banks; the central banks must regulate the payment systems and ensure the protection of both buyer’s information. According to (Taddesse and Kidan, 2005) there are legal issues associated with the global nature of e-payment; for instance, it may be tedious to establish the related laws to debated cases and the competence of certain jurisdictions. The execution of an e-payment system requires the establishment of legitimate administrative structures that builds trust and confidence.

Socio-Cultural-related Issues

The social-cultural differences and the use of various forms of cash (credit cards in North America and debit cards in Europe) have significant impacts on the establishment of a globally-relevant EPS (Taddesse and Kidan, 2005). As stated by (Taddesse and Kidan, 2005) the differences in the security level required and the productivity among various individuals complicates the issue. The buyer’s confidence in the conventional payment system makes it more challenging to embrace new ideas. New ideas may have no influence in the global market until customer’s privacy is ensured and security is confirmed (Taddesse and Kidan, 2005). Such new ideas must also be up to standard to attract people’s trust irrespective of
whether it is a simpler method or less expensive compared to the established methods (Kumaga, 2011).

Security of EPSs

Data and information security is paramount in all information systems (Khidzir et al., 2018). Data security in terms of the methodology, practices and technology involved to ensure data security is presented in Figure 1.

i. Unintended alteration or change (integrity).
ii. Unapproved access (confidentiality).
   i. Easily accessible to the approved clients based on demand (availability).

Fig. 1. Depiction of Information Security (CIA)

These security features are necessary in an e-payment system; an insecure EPS will lose client’s trust which is necessary to ensure acceptance. As stated by (Fekadu, 2009) there are security issues with e-banking and e-payment systems since they depend on basic ICT platforms which are prone to several economic and business vulnerabilities.

Security Demands in EPSs

There are certain requirements which must be met by any electronic payment system, such as:

Integrity and Authorization

1878
The integrity of a system may be described as its accuracy, validity, and completeness based on business qualities and desires. Integrity in payment systems implies that a client will never be billed unless his approval is confirmed. Furthermore, sellers must not accept any payment unless the client approves it (Asokan et al., 1996).

**Confidentiality**

Confidentiality is defined as the security of sensitive materials from unauthorized declaration. Few organizations have confidentiality as a part of their dealings. In this setting, confidentiality implies the secrecy of data information related to any form of transaction. Commonly, clients are interested in the security of their transactions (Dwork, 2018). When there is a need for anonymity, there may be a need to divulge such information to a certain group of the participants.

**Availability and Reliability**

Availability guarantees the existence of data frameworks and information when they are needed; it requires a regular communication of the amount of time a framework can be used efficiently. All aspects of the system must be ready to make or get payments whenever there is a need (Dwork, 2018).

**Enhancing EPS Security**

As per (Taddesse and Kidan, 2005; Hamza et al., 2018; Hashim et al., 2018; Handley, 2018; Cohen et al., 2018) the commonly used strategy for ensuring the security of EPS is by using hiding-based electronic systems such as encryption, steganography, watermarking, and digital signatures as explained in Figure 2. On application, these innovations have reduced money theft and forgery. Here, a brief explanation of the mentioned security methods that secures electronic payments is presented:
The advent of the Internet revolutionized e-payment; meanwhile, there is a challenge of securing information over open connections. To solve the information security problems, several techniques have been advocated in the area of security systems as depicted in Figure 2. Cryptograph or information encryption is a process of scrambling information in a manner that it becomes unattractive to an intruder. Meanwhile, electronic payment information may sometimes be difficult to encrypt. Therefore, there is a need for an invisible mode of communication which keeps the existence of a secret information from anyone. This is the reason an information hiding technique is required. There are two subdisciplines in information hiding, steganography and watermarking (Hussain et al., 2018). Both methods ensure the hiding of secret message and are related to each other through with different objectives. Steganography primarily aims at the hiding of the existence of secret communication and the protection of the secret information. Contrarily, watermarking aims at protecting the secret data integrity with or without hiding the existence of secret information from invaders. Watermarking applications mainly aims to protect the content’s intellectual property. Table 1 portrays the basic features of information encryption and information hiding techniques.
Table 1: Basic features of information hiding techniques

<table>
<thead>
<tr>
<th>Comparison criteria</th>
<th>Information hiding</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cryptography</td>
</tr>
<tr>
<td>Objective</td>
<td>Content protection.</td>
</tr>
<tr>
<td>Perceptual Security</td>
<td>No security as it can be easily identified (visible).</td>
</tr>
<tr>
<td>Communication security</td>
<td>The communication security is dependent on the key confidentiality.</td>
</tr>
<tr>
<td>Robustness</td>
<td>It is robust against the complexity of the ciphering framework.</td>
</tr>
<tr>
<td>Key requirement</td>
<td>A key must be used.</td>
</tr>
<tr>
<td>Type of output</td>
<td>The output is either the ciphertext or the plaintext depending on the medium.</td>
</tr>
<tr>
<td>Limit of security</td>
<td>Secure until the decrypted ciphertext loss its watermark.</td>
</tr>
<tr>
<td>Medium or</td>
<td>Any digital data</td>
</tr>
<tr>
<td>Carrier</td>
<td>Can serve as a carrier.</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Imperceptibility</td>
<td>It has a high imperceptibility.</td>
</tr>
<tr>
<td>Applicability</td>
<td>Has a universal applicability.</td>
</tr>
<tr>
<td>Capacity</td>
<td>It has a high embedding capacity, but long messages can raise its chances to be decrypted.</td>
</tr>
<tr>
<td>Detection method</td>
<td>It has an untargeted detection method.</td>
</tr>
<tr>
<td>Complexity of detection and extraction processes</td>
<td>The detection process is easy while the extraction process is complex.</td>
</tr>
<tr>
<td>Output data testing parameters</td>
<td>The use of parameters is optional.</td>
</tr>
<tr>
<td>History</td>
<td>It is a modern technique.</td>
</tr>
<tr>
<td>Drawbacks</td>
<td>Its problems include key management and the complexity of the encryption schemes.</td>
</tr>
<tr>
<td>Techniques</td>
<td>The available</td>
</tr>
</tbody>
</table>
techniques are the symmetric and asymmetric techniques.  

<table>
<thead>
<tr>
<th>technique is the spatial domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>technique is the spatial domain.</td>
</tr>
</tbody>
</table>

**Cryptography**

This is a conventional approach towards ensuring the privacy of transactions between two parties during an e-payment process (Baar and Walters, 2018; Abadir et al., 2017; Chaudhry et al., 2016). Cryptography refers to the art of secret writing in which a plaintext is encrypted into a ciphertext with a key before being transmitted through an insecure channel. The ciphertext can only be decrypted to the plaintext version using a valid key (Radwan et al., 2016) without which it will be impossible to retrieve the plaintext. Cryptography is a significant tool in ensuring a secure communication over an insecure channel because it confers privacy, confidentiality, non-repudiation, authentication, and key exchange. A cryptographic system is depicted in Figure 3 (Yassein et al., 2017). Data security can be ensured using two types of cryptographic schemes. These schemes are mainly used to achieve certain aims such as public/secret key cryptography and hash functions. The type of encryption algorithm used determines the length and type of the secret keys to be used (Yassein et al., 2017).

**Fig. 3. A general Scheme of cryptography**

![Cryptography Diagram](image_url)

**A. Symmetric/secret key cryptography:** This form of encryption is also called shared key, single-key, or private-key encryption. Private Key technique is used to encrypt data on all sides and must be used to decrypt the encrypted data. The sender encrypts the original data or plaintext with a key and transmits the secret key to the sender for the retrieval of the plaintext. This secret key is only available to the authorized persons during the encryption/decryption, Symmetric process depicted in Figure 4 (Yassein et al., 2017).
Although this technique provides a good level of transmission security, there is still a problem of the secret key distribution. Exposing the secret key to an unauthorized person will ruin the encryption process. The DES algorithm is a perfect example of a symmetric key framework (Yassein et al., 2017).

**Fig. 4.** Symmetric cryptography process

---

**B. Asymmetric/public key cryptography:** This technique can also be called an asymmetric or public key cryptosystem. In this technique, two mathematically-related keys are used for a separate encryption and decryption of data. When a private key is used in this technique, it is difficult to obtain the data and for this technique to proceed, all the keys are needed. The encryption key is publicly stored and as such, is referred to as a public key; the decryption key is secretly stored and as such, is referred to as a private key, figure 5 explains the process of Asymmetric cryptography process. The RSA is an example of an asymmetric key framework (Yassein et al., 2017).

**Fig. 5.** Asymmetric cryptography process
Steganography

This is an act of concealing and transmitting secret e-payment information through a reliable channel in a bid to hide the presence of the secret data. It ensures that there is no evidence of the existence of such message. It keeps the existence of the secret information in the cover message from the public, thereby, keeping the information safe and free from any retrieval attempt. An overview of a steganographic system is depicted in Figure 6 (Yassein et al., 2017). The secret data can be embedded in a cover media using a stego-system encoder without the need for an algorithm. Anything that can be represented as a bit, such as a plaintext, a ciphertext, or an image can be embedded using this method. Having embedded the secret data in the cover object, the resulting carrier is called a stego-object which is transmitted to the intended destination via a suitable channel. Upon receipt of the stego-object, a decoder system is used with a similar stego method to retrieve the original data (Yassein et al., 2017). There are different types of steganographic methods based on the digital carrier used as follows (Figure (7)).

**Fig. 6.** The principle of steganography

- **A.** Text steganography: In this method, text files serve as the cover object. The secret data is embedded in every n<sup>th</sup> letter of each word in the text file. There are currently
many available methods in this category, such as Format-based method, Linguistics method, and Random and statistical method (Hashim et al., 2018).

B. Image steganography: Here, attractive cover objects are used to embed the secret data. The secret data is embedded using message pixel intensities; images are mainly used as the cover object due to the presence of several bits in a digital image representation (Gupta and Bhagat, 2019).

C. Audio steganography: Audio files are used in this method to hide a secret message. Some of the commonly used cover objects are WAV, AU, and MP3 sound formats. Some of the methods used in audio steganography are Low Bit Encoding, Spread Spectrum, and Phase Coding (Zhang et al., 2019).

D. Video steganography: Files in video formats are used in this technique to hide secret data. Some of the commonly cover objects in this method are AVI, H.264, MP4, and MPEG video files (Dalal and Juneja, 2018).

E. Network or protocol steganography: Here, network protocols like TCP, UDP, ICMP, IP etc. are used to hide data in the cover object. In the OSI layer network model, there are secret channels which can be explored for steganographic purposes (Abbas, 2018).

F. DNA steganography: This method exploits the randomness feature of DNA to conceal secret data. It is a recent technique used for the numerical mapping of DNA sequence and has been explored for secret data embedment (Vinodhini and Malathi, 2018).

Fig. 7. Steganography digital carrier

Related Work

An algorithm for the detection of fraud in credit cards called BLAH has been proposed by (Babu et al., 2014). This algorithm is a combination of BLAST and SSAHA frameworks. These frameworks are proficient algorithms for sequence alignment and detection of frauds in
credit card. The system called BLAHFDS detects fraudulent transactions using a profile and deviation analyser. These analysers detect fraud using BLAH as a tool for sequence alignment. The proposed model was suggested for the generation of synthetic transactions to analyse the performance of BLAHFDS. This system presented a good fraud detection performance with a high accuracy. It also resented a fast processing speed but cannot detect cloned credit card or duplicated transactions. Fraud in other sectors such as telecommunication can be countered using BLASTSSAHA hybridization approach.

An FDS which combines the result achieved from the present and past behaviour of a user has been proposed by (Panigrahi et al., 2009). There are four elements in this fraud detection system (FDS), which are Rule-based filter, Transaction history database, Dempster–Shafer adder, and Bayesian learner. The doubt level in each transaction is extracted by the Rule-based Filter based on its variation from the normal spending pattern. The Dempster–Shafer adder combines all the doubtful transaction obtained by the Rule-based filter to establish a primary belief. The Hidden Markov Model (HMM) is a common statistical tool used to solve several problems.

Ashpan et al modelled the sequence of operations involved in credit card transaction processing using HMM. They considered the relationship between the transition probability and the hidden state and observations (Babu et al., 2014). Sasirekha et al suggested an Intrusion Detection Systems (IDS) which combines anomaly, misuse, and decision-making models to achieve a decreased rate of false positive alarms and a better detection accuracy. The HMM approach can be used to build an integrated IDS to detect attacks in credit card system based on the anomaly detection module. The behaviour of the card holder is considered as attributes and suspicious transactions are detected from the user’s spending profile. Suspected illegal transactions are then forwarded to a misuse detection system.

In another study (Lee et al., 2015) the author stated that trust is very important in online e-commerce environment as it determines customers preparedness to participate in an online transaction system. Digital certificates and signature are commonly used in controlling or avoiding risks of fraud and for securing online-based transactions (Lee et al., 2015). In other study (Sneha and Prachi, 2016), the author explained e-commerce for goods and services during online transactions. It was observed that protection policies that ensures security and re-liability over companies providing services are the barriers to online shopping services. However, consumer’s responses towards online purchase includes concern over sharing of sensitive personal information, unsolicited contacts from the online shopping system, and tracking of shopping activities (Roy and Venkateswaran, 2014). Besides system security, consumers are also concerned about illegal bridging devices that are technologically protected to acquire consumers personal, financial or transaction-related personal
information. Concern is also raised for information sharing with online payment retailers, as well as fraud due to a purposeful non-delivery of goods already paid for which are among the potential threat to online shopping. Improved security model for online purchase could minimize customer’s misbehaviour with the introduction of online transactions (Chen et al., 2011). Disposing of the customers banking details and card details during and after online transactions should be avoided as it is prone to illegal use and misuse. Once an information is revealed, an attacker can misuse it for other purposes. Online payment system could be improved by introducing policies that are technically sound, incorporate legal, rigorous standards for security of data or information, and with the issue of certificate from trusted third parties (Chen et al., 2011). In another study (Hu, 2011), the author enhanced the security of online shopping system to encourage consumer’s engagement in online shopping or e-commerce as well as to create awareness among Libyan economic units. Consumers feel confident and relaxed while using online medium if their capital and personal information are properly protected and secured (Hu, 2011). In addition, online portals should include elements that encourage trustworthy relationship between customers and online portals in order to improve the purchase of goods and attract customers. The portals should also ensure that every transaction is based on agreements that must be fulfilled (Premkumar and Narayanan, 2012). The protection of the customer’s data and security can bring awareness and trust to Libyan economic units.

The impact of information security for e-businesses was discussed by Eben with emphasis on the potential losses and security threats that could result from these vulnerabilities. The security of e-business consists of 6 dimensions which are confidentiality, integrity, legitimate use, auditing, availability, and non-repudiation. The study advocated for the designing of a systematic and comprehensive security policy that will ensure business security (EbenOtuteye, 2003). Cheng, Hamid, and Cheng (2011) suggested 5 perceived security risks as physical, performance, time, psychological, and financial loss. Physical risk includes cash or card loss while performance risk includes the risk of additional charges when used. Psychological risk involves risks that will affect the perceived image of the user when such payments are made; time loss risk involves risks due to a prolonged process time compared to an alternative mode of payment. Financial risk involves activities that will invoke non-refundable financial loss if performed. Srinivasan (2004) believed that the success of e-businesses depends on several factors. He stated that e-businesses must strive to develop trust over a period. According to the author, some of the factors that contributes to gaining customer trust include product or service offerings, appeal of the Website, branding, trusted seals, and quality of service. Trust can be considered in many perspectives, such as information content, product, transaction, technology and institution. In this paper, the author analysed trust from the transaction point of view and highlighted measures that e-businesses
must take to build customer trust. It is not easy to measure factors that contribute to trust because it is developed over time. People always rely on their past experiences to trust a business; they also depend on third party reviews and recommendations. The study concluded that e-businesses can be accessed from anywhere at any time but there are certain factors that impedes building and maintaining trust. The major problem of this study is that it failed to focus much on the ways a company can improve online security during transactions. Perea y Monsuwé, et al. suggested a framework for the improvement of researcher’s understanding of the attitude of consumers toward online transactions in the US and Europe. The framework deploys the Technology Acceptance Model (TAM) constructs as a basis and extended its external factors and applied it to the online shopping context. The review portrayed that customer’s attitudes toward online transactions are not only affected by usefulness and ease of use of the platform, but also by external factors such as consumer traits, product characteristics, situational factors, past shopping experiences, and trust in online transactions (Perea et al., 2004). Abdul et al assessed the impact of security and trust on the consumer’s willingness for online transactions among the urban Moroccans. This study examined customer’s preparedness to shop online by considering demographic factors, trust and security related factors. From the logistics regression analysis performed, customer’s willingness to participate in online shopping was found to be reliant on trust, security, age, awareness and piracy factors. The study also found that most of the respondents are willing to shop online. The result of this study was undoubtedly important to both online vendors and the government for a better understanding of online shoppers. The outcome of the study also encouraged decision-makers to develop better online shopping facilities with the technological competitive advantage for both online shoppers and vendors (Tariq and Eddaoudi, 2009). The economic impact of e-banking in Bangladesh was studied by Baten and Kamil; they also studied the benefits and scope of e-payments in Bangladesh (Baten and Kamil, 2010). Furthermore, Salehi and Alipour studied e-banking in an emerging economy with the aim of seeking to provide empirical evidence from Iran (Auta, 2010). James investigated the acceptance of e-banking in Nigeria using Statistical Package for Social Sciences (SPSS). The study outcome e-banking acceptance to depend mainly on the age, income, educational status, perceived benefits, perceived risks, and perceived ease of use (Odumeru, 2012).

Conclusion

The significance of electronic payment systems in global trade and commerce is quite evident from the changing modern trends. Their scope ranges from one-dollar transactions to several million-dollar transactions. This study gives a wide knowledge of electronic payment systems and payment security considerations. A secure electronic payment system for online shopping
is proposed by using information security systems like steganography or cryptography or by a combination of both techniques to protect customer’s data and minimize misuse or fraud at the merchant’s side. Considering the previous studies, it is possible to gain valuable knowledge about the pros and cons of the currently available electronic payment systems and the available security mechanisms for electronic payment systems. This paper also analysed electronic payment systems from different security perspectives with the aim to provide a better customer understanding and satisfaction.

REFERENCES


1891


Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017, August). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Engineering and Technology (ICET), 2017 International Conference on (pp. 1-7). IEEE.


Sneha M. Shelke, Prof. Prachi A. Joshi , A Study of Prevention of PhishingThreatsusingVisualCryptography,2016


EbenOtuteye (2003). A Systematic Approach to E Business Security: Faculty of Administration,


University of New Brunswick, Fredericton, Canada,