5-10-2022

Exploring Digital Checking: Evolution, Technology, and Future Directions

Mohammed Hasan Saleh Bamasood

RIT

Exploring Digital Checking: Evolution, Technology, and Future Directions

by

Mohammed Hasan Saleh Bamasood

A Capstone Submitted in Partial Fulfilment of the Requirements for the

Degree of Master of Science in Professional Studies:

Smart Cities

Department of Graduate Programs & Research

Rochester Institute of Technology

RIT Dubai

May 10th, 2022

RIT

Master of Science in Professional Studies:

Smart Cities

Graduate Capstone Approval

Student Name**: Mohammed Hasan Saleh Bamasood**

Graduate Capstone Title**: Exploring Digital Checking: Evolution, Technology, and Future Directions**

Graduate Capstone Committee:

Name: Dr. Sanjay Modak **Date:**

Chair of committee

Name: Dr. Khalil Al Hussaeni **Date:**

Member of committee

Acknowledgement

The realization of this capstone project would not have been possible without the kindest support, professional advice, and ardent motivation offered by Dr. Sanjay Modak and Dr. Khalil Al Hussaeni. I also would like to acknowledge all the assistance related to the theories and methodologies suggested by Mr. Ammar Harbah, Senior Statistical Analyst, and Mr. Rabeh Sodki, Economical expert at Digital Dubai. I also appreciate my colleague Mr. Ali Abdullah, Branch manager at Emirates Islamic, for his support in introducing the recent developments in the world of banking practically, as well recommending some references that would support the project.

Words are not enough to express my profound appreciation for the time shared with me while preparing for, researching, gathering literature and relevant theory, and writing the capstone project.

From my heart, please accept my sincerest appreciation and gratitude for all the help extended to me in the completion of this project.

Abstract

This capstone project sought to explore the evolution of digital/electronic checking, assess how technology and other factors fueled the development of digital electronic checking, evaluate if the sampled research literature indicate that the desirable attributes of a payment instrument have been fully addressed; and analyze issues that deter the digital/electronic checking system to fully integrate the six most desirable attributes for a payment instrument in order to recommend possible directions for future research and design implementation. The project utilized integrative review as its methodology and adopted a theoretical framework based on the input-process-output model to guide the analysis and presentation of deliverables. Ten research articles from relevant journals were sampled to represent the about two decades of development of digital checking as well as supporting theory from authoritative sources. The findings revealed that cryptography was a dominant technology in the evolution of *e*-checking, which facilitated the role of human ingenuity as motivation for innovation and development of more efficient systems. Additionally, the gap in knowledge and practice, to date, in digital/electronic checking concerns fraud and other technology-enabled security threats. Recommendations to address security threats which prevent wide adoption of *e*-checking point towards biometrics, quantum cryptology, and a blend of data mining and artificial intelligence, specifically deep learning and neural networks. It is also essential that programmers and other information/wireless security professionals remain vigilant about the implications of legal aspects and human rights in the implementation of technological solutions to security threats.

Keywords: Digital checking, *e*-check, electronic check, evolution of technology, fraud detecting technology-enabled security threats.

Table of contents

List of Figures

Statement of the Problem

A *check*, also spelled as *cheque* in British and French territories, refers to a signed paper document which instructs the signatory's bank to pay to the designated payee an amount of money by deducting the amount from the signatory bank account after a specified date (Anderson, 1998). The idea behind what the financial industry regards in modern times as the check may be traced back to the first millennium from the eastern Mediterranean region, where local merchants regard today's check as a convenient mode of payment. Eventually, with the development of the check's negotiability during the 16th century, checks also turned out to be a more versatile payment instrument in Europe (Quinn & Roberds, 2008).

As paper checks continue to evolve into electronic or digital checks, it is worth noting that the all-electronic check can be designed with the six most desirable attributes of a payment instrument: certainty, convenience, economy, information, security, and universality (Jacob et al., 2009). *Certainty* entails a nominally reasonable processing time and a strong legal framework which distinctly specifies and ensures how and when value exchange takes place between the payor and the payee. Meanwhile, *convenience* refers to the non-arduous conduct of payment activities in terms of initiation, receipt, and dependable record creation and maintenance. On the other hand, the attribute *economy* is concerned with acceptable and reasonable transaction costs of maintenance and operation of the digital checking in terms of the effort used up in completing transactions. Information, as an attribute of a desirable mode of payment involves the specific knowledge and familiarity of users in the processing and recording of transactions, easily recognizable payee identification, and infallibility of authentication, as well as the availability of information sources. The attribute *security* deals with the protection afforded to the transfer of

value and the supporting identity of transaction participants from breach of data and fraud. Finally, *universality* suggests wide acceptance of the payment instrument by banks and a substantial majority of payors and payees, bolstered by the availability of a reliable infrastructure Jacob et al., 2009).

Research Questions

Three research questions are proposed as focus of the analysis in this capstone project:

1. How did digital checking system evolve technology-wise?
2. What factors influenced the development and advances in the digital checking system?
3. In what direction is the future of digital checking technology headed in terms of addressing emerging technology-enabled security threats?

The first and second research questions were formulated to ascertain which among the six most desirable attributes of a payment instrument are now embedded in today's digital checking system. The first research question explores the flow of electronic checking system development based on the technology implemented in system design. Meanwhile, the second research question assesses the factors which drove the development and advances in the digital checking system and identify which among the desirable attributes have not yet been fully addressed, to date. Finally, the third research question ventures to solve the current issues which currently best today's digital checking system based on research literature and emerging theory and recommends possible directions for future research and/or implementation of more robustly designed digital/electronic checking systems.

Background of the Problem

Earlier attempts to shift from traditional to electronic checking were spearheaded by legislation, particularly in the United States, by a cooperation among banking institutions like the Automated Clearing House and later, through legislation, to fortify policies and procedures for the envisioned essence of the shift via electronic check presentation initiative and the Check Clearing for the 21st Century Act.

The ACH

One of the earlier attempts to shift check payments to electronic method or the *e*-check in the United States, is the Automated Clearing House (ACH), instituted in the 1970s by commercial banks with the Federal Reserve designated as operator (Humphrey & Hunt, 2012). Such shift to electronic checking came in slightly later in the UK and Europe (Carrera, 2020). The ACH functions to process check payment information and transmit the data electronically among the various check clearinghouses, which facilitated collection, minimized the cost of both processing and delivery. However, the ACH grew slowly, where a possible explanation could be the proliferation of billers who accept payments through preauthorized ACH debit (as direct debit) to the payor banks. Accordingly, check payees consisting of employees, retirees, Social Security recipients and other payment and payroll recipients, but most especially overnight bank transactions involving corporate cash management activities (Humphrey & Hunt, 2012).

For the most part, banks accumulate daylight and idle balances from corporate customers of various banks and channel these for sale into the overnight market or the following day for corporate uses, such as in funding subsidiary operations, and in the process, earn interest return. The slow growth of ACH may be attributed to the challenges in obtaining customer authorizations which allow both collectors and disbursers to automatically debit or credit their

clients' deposit accounts. Another factor which contributed to the slow growth of ACH was a provision in the Uniform Commercial Code, which allows the payor bank to receive and scrutinize the physical check before release of the payment. Over time, checks have been replaced by ACH debits and credits for bill payment and payroll, respectively and other recurring income transfers. Other merchants also use ACH electronic debit at the point of purchase from the client's deposit account or use check conversion at the back office instead of the cash register (Humphrey & Hunt, 2012).

The ECP

The Federal Reserve instituted the electronic check presentment (ECP) in the 1990s as another banking sector initiative to migrate paper checking to electronic checking, with practically the same goals as ACH, which are to render check payments faster and reduce the unit cost of processing the payments (Humphrey & Hunt, 2012). The principle of ECP is practically the same as the later implementation of ACH through accounts receivable conversion (ARC), back-office conversion (BOC), and point of purchase (POP). The basic difference was the separate electronic transmission of the check amount to the payor's bank and truncation of the paper check at the sending bank instead of the check amount ACH debited and encoding of the bank number and the depositor account number (also known as the MICR line). Check processing costs were also reduced with the ECP as 25% of checks are deposited and electronically presented by way of ECP (Humphrey & Hunt, 2012).

Check 21

Check Clearing for the 21st Century Act (Check 21) was more successful than the ACH because it was reinforced by a legislation which rendered the image of the substitute check legally similar as the physical check (Humphrey & Hunt, 2012). Check 21 eased the movement

of checks in the payment system permitting smoother transport of check images between banks electronically. It was considered by legislators as an innovative step towards modernization of the system of check transportation as an interim measure for the electronic movement of checks in the financial system. The reduced processing time for issued checks to be deducted from the payor's account have resulted to savings up to two billion dollar each year in processing costs. However, as of 2006, only about one percent of the checks are cleared electronically (US House of Representatives, 2006).

Despite the advantages and innovation instituted by Check 21, one of the issues working against the legislation is the cost of the equipment for check truncation and electronic imaging which will cost the banking sector around 10 billion dollars over the next five to seven years (McGlinn, 2005). The legislation also waived the right of checking account holders to demand the original checks they issued, but instead demand/request for the substitute check to benefit for the right to recredit. Additionally, Check 21 does not prohibit banks from charging higher fees for checking accounts for back-issuance of substitute checks (McGlinn, 2005).

The pioneering design for a functional online electronic checking system was introduced by Chaum et al. (1990 a, b) in 1988, and in 1989 an offline system was also presented. It was about a decade later when the very first *e*-check was issued by the United States Treasury Department to the Department of Defense in the maiden implementation of the Electronic Check Project under the auspices of the Financial Services Technology Consortium (Anderson, 1998). Given that the more practical electronic checking system is the online version, the strengths of an online checking system co-exist with a host of cybersecurity and related risks. The major security issues in the implementation of e-checks comprise of adequacy of security measures, data leaks, as well as forgery and content alteration (Li, 2015).

Objectives and Deliverables

Objectives

The objectives of the capstone project, as reflected in the title are to: (1) explore the evolution of digital/electronic checking in terms of the technology implemented in design and programming; (2) assess how technology and other factors fueled the development of digital electronic checking and evaluate if the sampled research literature indicate that the desirable attributes have been fully addressed; and (3) analyze issues that deter the digital/electronic checking system to fully integrate the six most desirable attributes for a payment instrument and recommend possible directions for future research and design implementation, based on research literature and emerging theory.

Deliverables

The capstone project deliverables include the following: (1) a flowchart which depicts the development of digital/electronic checking pertaining to the sampled literature from Chaum et al. (1990a) in 1988 to Sertkaya and Kalkar (2021), in phases, based on the dominant technology utilized in system design and the various methodologies applied for each phase to summarize the results for the first research question; (2) an illustration through an image of the extent of integration or strength of the six desirable attributes of a payment instrument for digital checking; and (3) a set of suggestions and or recommendations of newer technologies or emerging theories which may be applied for the banking sector in particular and the global financial services system to fully benefit from the six most desirable attributes identified in Jacob et al. (2009) for a payment instrument.

Literature Review

This section surveys and summarizes ten research articles pertaining to digital/electronic checking in sufficient detail to establish the groundwork for the three deliverables identified in the preceding section. The research articles are presented in chronological order from 1988 to 2021 in order to facilitate classification of the development of digital/electronic checking into phases, as well as identify the key technology and procedure applied for each phase. If necessary, the review will be supplemented by additional literature and theory in the discussion of results and presentation of deliverables.

Untraceable Electronic Cash: Precursor of the e-Check (1988)

The authors, Chaum et al. (1990a) were either too modest to mention in the expanded abstract or they have not yet realized that their 1988 work (i.e., published in 1990) initiated the basic concept of an electronic check. However, with their pioneering work to address both anonymity and accountability in Chaum et al. (1990a), their monumental work in 1988 on electronic checking also paved the way for a more recent development in the financial sector – blockchain technology, where the bitcoin was implemented only in 2009 (Sharma et al., 2021). However, the "philosophies from various electronic cash or digital cash paved the way for cryptocurrencies in general and bitcoin in particular" (Sharma et al., 2021, p. 187).

Chaum et al. (1990a) highlighted that electronic cash generation should be facilitated with the cooperation of the bank(s) and recommended a protocol for issuing and spending electronic cash using a fictitious payor designated as "Alice" as it introduced the RSA digital signature discussed later in the literature review.

The protocol has a number of advantages: simple verification regarding the appropriate structure of the electronic cash and corresponding signature/acknowledgement by the bank, but

the bank will not be able to associate the cash to the account of Alice. The protocol also does not require the shopkeeper to get in touch with the bank for each transaction. Hence, Alice's privacy remains unconditionally protected for as long as she uses the electronic cash only once. However, the protocol is able to detect if Alice reuses the electronic cash and will be able to link the cash to her account and render her accountable for using it twice (Chaum et al., 1990a).

Untraceable cash. For electronic cash/coin to be untraceable, an RSA modulus, n is first published by the bank, as well as the security parameter, k. The factorization of n is kept secret, and the expression 9(n) has no small odd factors. In addition, Chaum et al. (1990a) also discussed a possible problem and the corresponding fix when Alice is involved in a collusion with another shopkeeper, say Charlie, such that Alice describes the transaction to Charlie after the transaction with Bob. When the bank receives the information from both Bob and Charlie, it detects a high probability fraud in one of the transactions, but is unable to pinpoint which one is the fraud and will not be able to trace it to the account of Alice. The fix devised by Chaum et al. (1990) is an anti-fraud coalition, where shopkeepers provide a *fixed query string*, with every two strings at *Hamming distance* of at least *ck* for the constant *c*. A *query string* is described as a set of query elements together with the "g" and "|" Boolean operators, where *fixed query string* may be written as optional "+" or "–" sign, and followed by one or more decimal digits with an optional decimal point (Schmidt & Brodie, 2011). Meanwhile, *Hamming distance* is the number of elements in which two codewords are different (Kim, 2015). Hence, to disallow Alice from reuse of the same electronic cash at the same shop, the challenge is kept random or shopkeepers need to maintain their own list.

On multiple spending, untraceable checks, and blacklisting withdrawals. One limitation of the Chaum et al. (1990a) protocol is the possibility of the bank framing Alice as a

multiple spender, which suggests that the protocol described did not seriously consider legal significance. Rather, the protocol simply assumed that Alice has the benefit of a digital signature and a certified public key. Hence, Alice is computationally, but not unconditionally protected from the sequences of a bank multiple spending frame-up on the assumption of her digital signature, but her privacy is unconditionally protected.

For untraceable checks, Alice can generate several checks with one bank interaction. These checks are similar to those described in the previous subsection. However, to disallow multiple spending using one check by Alice, j factors encode the purchase sum and $k - j$ factors prevent multiple spending. The bank then publishes two different RSA moduli n and n' to represent two digital signatures, letting v as Alice's personal check counter. Alice sends the bank several t pairs of major and minor candidates, but blinds the major and minor terms before sending them to the bank. Then, Alice can make a purchase by encoding the purchase sum considering the first j as denominations 1, 2, 3 …'s (j –1) and reveal the y term to the shopkeeper. However, the last $k - j$ disallows Alice from using a check more than once. It is also important if shopkeepers will be able to present a random challenge or shopkeepers maintain a probe sequence for $k - j$ terms selected from a code with a big Hamming distance. Moreover, to be able to blacklist electronic cash used more than once, the bank encrypts redundant terms in Alice's random selection, which the bank recognizes when a check is spent more than once. However, this part of the protocol provides privacy protection to Alice only computationally, but not unconditionally (Chaum et al., 1990a).

Efficient Offline Electronic Checks (1989)

The seminal work of Chaum et al. in 1988, but published in 1990 was acknowledged as the precursor of today's online checking system, but they acknowledged in their research report

that protocol they devised was not perfect (Chaum et al., 1990a). Hence, the following year, they released an improved version of their previous protocol, which they described with more advantages including unlinkable and anonymous withdrawal and payment capable of saving 91% of the signatures, and mathematical operations, such as 41% of the other multiplications, 73% of the divisions, and 33% of the bit transactions (Chaum et al., 1990b).

The other advantages of the improved system are: capability for the payor to refund a number of checks at once to keep the bank from learning the face value of each check; check withdrawal and payment are unconditionally unlinkable provided that the check is not spent twice, otherwise, the fraud can be link to the payor's account; no computations need to be made by the payor; no need for online connection of the shop with the bank; one signature per payment by the bank; payments and refunds are unlinkable, but the bank is able to learn the total number of unspent denominations; refunds and withdrawals can also be made unlinkable (Chaum et al., 1990b). Like in Chaum et al. (1990a), the payor is also designated as Alice, who creates candidates in a special way. Based on the cut and choose protocol, the bank randomly selects some of Alice-designated candidates with the inner arguments of the selected candidates need to be revealed by Alice. This part of the protocol is required in order to prevent cheaters, such that either there are not too many bad candidates left (i.e., candidates created the proper way) or to be able to obtain the same security when more checks are withdrawn at one time, less candidates need to be opened. Given that that the payments are anonymous, check are bought for the maximal amount, such that the bank signature is split for the payment and the refund part (i.e., for refund of the unspent value) (Chaum et al., 1990b).

Changes for improved efficiency compared to Chaum et al. (1990a). Three changes were made for improved efficiency:

(1) Alice does not initially send to the bank the candidates for the check, but rather the value of a one one-way function using the candidates as arguments, which avoids sending half the candidates to the bank;

(2) The terms used in the check are ordered, and thus, possible to have almost the same root;

(3) While Alice needs to send a blinded product of the major and minor terms, only one half of the blinding factors need to be sent, together with about just half as much bandwidth, and requires only one signature from the bank. However, upon receipt of the signed check, Alice had to separate the product of the minor terms signed to initiate the refund of the spent amount, and, therefore, had to perform some calculations. She must also initiate an additional one-way function to enable this change.

The modified payment system now requires 3 parties: the bank, the payor Alice and the shop. The system can facilitate four transactions not necessarily in the following: deposit, payment, refund, and withdrawal. Also, each transaction involves a protocol between two of three parties.

The Virtually-Defaultless Check System (2000)

Lee and Yoon (2000) designed a virtually-defaultless check system using intelligent agents and facilitated by the *SafeCheck* system. Prior to the new millennium, and as explained in Lee and Yoon (2000), an electronic version of a paper check system resembles that of an electronic fund transfer (EFT) or a credit card system. In EFT, money is transferred electronically from one account to another without any payment instruments, such as written checks or other procedures for collecting cash (Doshi, 2020). Once payments are electronically

mediated, there is considerable dependence on Internet service providers, telecommunications services and other technological utilities for the smooth conduct of activities. Additionally, EFT is exposed to such cyber risks as issues in transaction integrity, system hacking, as well as system unavailability (Doshi, 2020). In a limited sense, electronic or online checking resembles EFT in terms of the payee bank being presented the check by the payee (i.e., the drawee of the check issued) for clearing so that the transaction can be executed electronically (Lee & Yoon, 2000). In this similarity with EFT, online checking ceases to benefit from the merit of the courtesy of an overdraft check issuance extended by most banks to preferred clients.

Meanwhile, personal consumer credit card or charge account system involves a contract between the company offering the credit or charge account and the consumer (i.e., the account holder). Credit card holders charge purchases to the account at any time on the condition that all or part of the debt is to be paid each month, up to a maximum amount of debt at a time, termed as the credit limit. However, if the total amount of the credit owed is not paid at the end of a fixed period each month, a finance charge is added to the total amount owed by the credit card holder (Dlabay, 2018). Most credit card accounts assign an institutionally-designated clearing date as part of the revolving benefit of the credit, which according to Lee and Yoon (2000) renders electronic/online checking similar to the credit card system. However, electronic/online checking is fundamentally different from the credit card system in terms of the frequency of authorization payment. In a credit card system, payment authorization is per transaction, whereas traditionally payment authorization through the check system on a checkbook level. This suggests that the checking system requires less effort in payment authorization which exposes it to a higher risk for default (Lee & Yoon, 2000).

The check system designed by Lee and Yoon (2000) was designed to benefit from the advantage of overdraft issuance on the payer's end, avoid the risk of default on the payee's end, and minimize the costs associated with payment authorization to guard against default risk. The *SafeCheck* system designed by Lee and Yoon (2000) in Figure 1 is an electronic check payment system to avoid or reduce default risk, lower payment authorization cost and allow credit-based payment. Selected scenarios are illustrated for functional check flow.

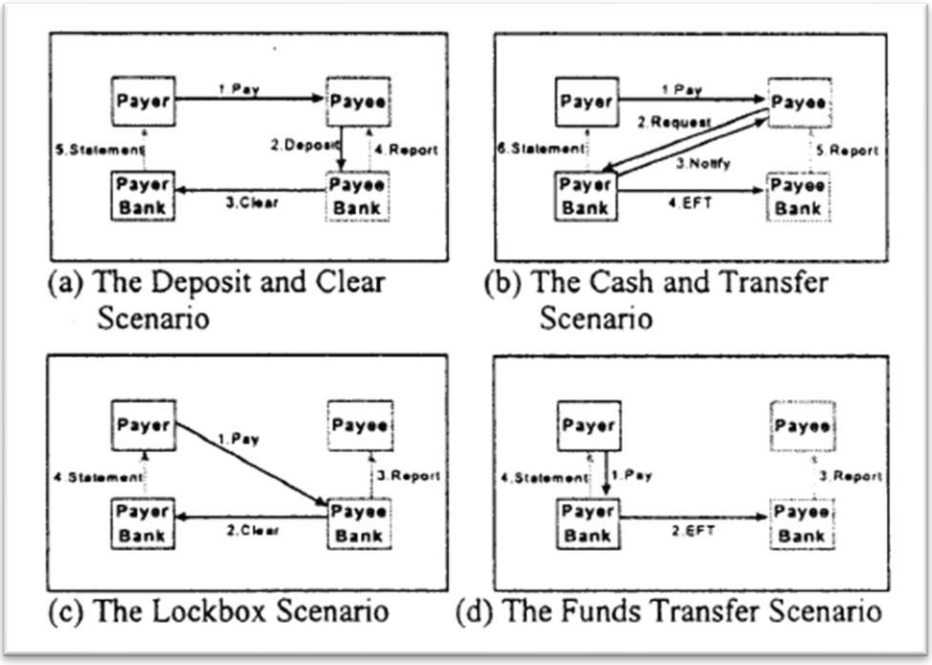

Figure 1. Selected scenarios depicting functional flows for electronic checking (Lee & Yoon, 2000, p. 226)

As reproduced in Figure 1 from Lee and Yoon (2000), four functional scenarios were proposed by the Financial Services Technology Consortium (FSTC). It can be observed that scenarios (a) and (b), namely the *deposit and clear* and *cash and transfer* scenarios, which involve the clearing process may not be completely safe from default risk. As a safeguard, n (c), when a variation of the EFT is instituted as part of electronic checking, where with the use of the *VirtualPin* system, the check drawn/requested by the payee is automatically withdrawn from the

payor's account as the check amount is approved and deposited to the payee's account (Lee & Yoon, 2000).

In Figure 2, the architecture of the *SafeAssign* system is presented with the following three agents: the checkbook and check receipt agents (in dashed circles) and the bank control agents (in dashed rectangles).

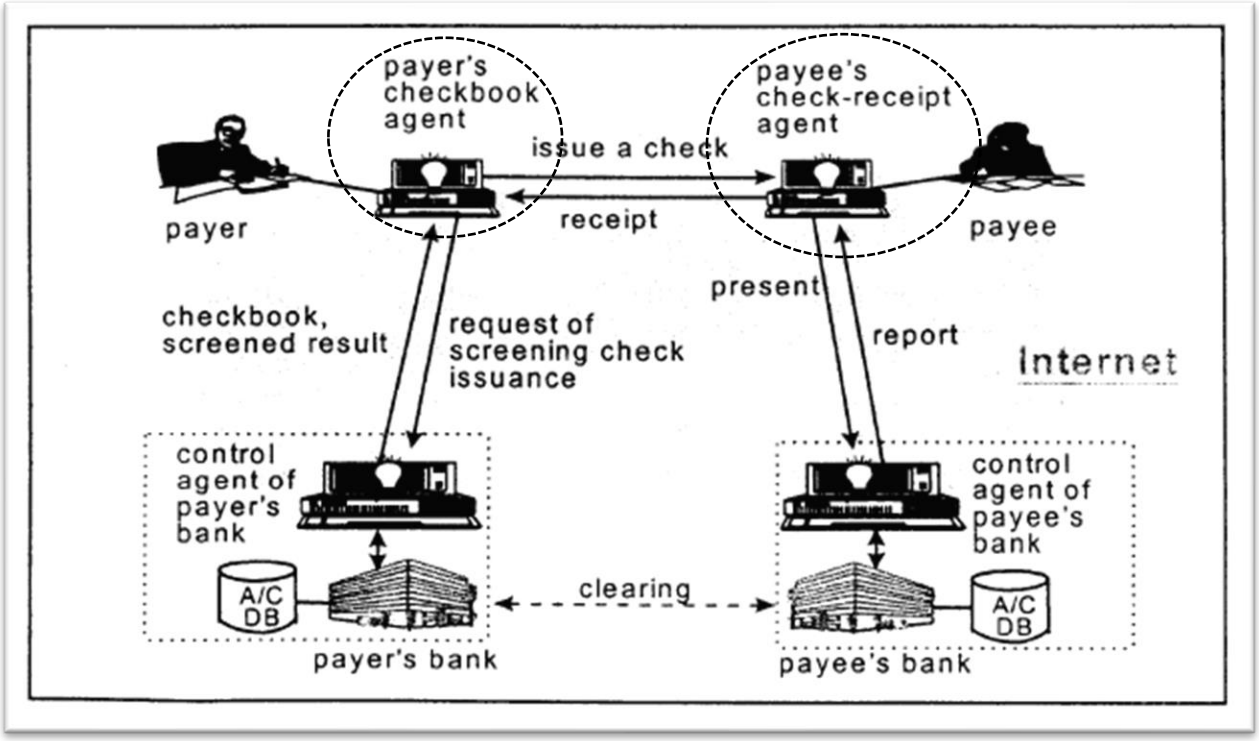

Figure 2. A schematic diagram of the *SafeCheck* system architecture (Lee & Yoon, 2020, p 226).

The architecture of the *SafeCheck* system in Lee and Yoon (2000) involves the deployment of three intelligent agents. Intelligent agents refer to "software components that can work autonomously and proactively to solve the problems collaboratively … can behave in a cooperative manner and collaborate with other agent consulting systems" (Challenger et al, 2021, p. 195).

Checkbook agent. The *checkbook* agent performs at least four distinct roles: opens the checking account, confirms the validity of check issued, receives instructions regarding the rule-based model, and keeps records of checks issued.

Check-receipt agent. The check-receipt agent also executes four tasks: evaluates the validity of the checks and return receipts, presents the paid checks, receives instructions regarding the rule-based model, and keeps records of checks paid.

Bank control agents. The bank control agents carry out a host of functions for the *SafeCheck* system designed by Lee and Yoon (2000), including: decisions to permit opening of a checking account and dissemination of the result accordingly, credit scoring of the checking account and decisions and notification of credit limit of each checking account, modification of the mode of the account including issuance of digital certificate or suspension, decisions about the number of blank checks and limit for the account, blocking of check issuance, authorization issuance for lower credit client, updating of account balance for checks cleared and periodic reporting of electronic/non-electronic withdrawals, provides notifications regarding rules modified, and issue digital certificates to customer agents (Lee & Yoon, 2000). On the whole, the SafeCheck system is virtually-defaultless because modifications were instituted via intelligent agents to check missed authorization for checks which are likely to be defaulted and block non-allowable issuance in a distributed manner. Hence, check issuance using the system is adjusted based on the issuer's credit eligibility.

A New E-check System (2004)

Liu et al. (2004) introduced two similar versions of e-checks systems where one version supports partial unlinkability and the other offers complete unlinkability but with a more complex setting. Both schemes were constructed as extensions of the *e*-cash system initiated by

Ferguson and both do not need a trusted party for efficient implementation. Ferguson's *e*-cash system utilized a single term for large set of possible challenges and the withdrawal protocol did not implement the cut-and-choose technique like other systems, but rather used direct construction (Ferguson, 1994). One modification of the protocol is that one of the signature pair (*a*) will have to be dependent on an additional one-way function comprising of the exponents (e_b and e_c), which tones done the freedom of the payor in obtaining signatures. Another modification is that the number *C* on the withdrawal protocol is given a random power in the first signature to disallow the payor from combining an old coin/*e*-check with one that is currently withdrawn, with the use of a random number, *k* (Ferguson, 1994).

Cut-and-choice vs. direct construction. Cut-and-choice refers to a two-party protocol where one party ventures to persuade another party that data transmitted to the first party was constructed honestly based on an acceptable method (Crepeau, 2019). Meanwhile, direct construction refers to the use of polynomials over finite fields, which satisfies the lower bounds of key-sizes with equalities, and is thus, regarded to be optimal (Seito et al., 2010).

E-check version 1. A list of reasonably large prime numbers is provided as the bank's public exponents, which is capable of representing an amount up to $\$2^k - 1$. The withdrawal protocol proposed in Lui et al. (2004) is very similar to Ferguson's proposed scheme. The devaluation $\overline{vd}$ of the payment protocol is always computable. The *e*-check is denoted as *K* and (*a*, *b*, *c*) are the check base numbers. To clarify, the prior division operation is the normal division procedure without taking the modulo. The check base numbers are then sent by the payor to the shop, where the shop randomly selects a challenge (*x*), which is eventually sent to the payor.

Deposit and refund protocols. In the first version of the Lui et al. (2004) *e*-check, the deposit protocol is similar to the work of Ferguson, except that checking for double spending had been incorporated. The bank then verifies the ownership of the *e*-check and after verification, refunds the remaining balance of the payor account and creates a report/record of the refund. Note that the bank can associate the identity of the user to the refund and can also link any instance of a double-spend to the payor.

E-check version 2. In version 1, the refund phase can be linked to the payor's account. In this version, unlinkability is achieved in all phases, where the bank only possesses one public exponent (v), but uses different elements for different values of the check. Hence, the maximum value of the *e*-check is maintained, and double-spending is also prevented. The only difference of the Lui et al. (2004) scheme with the Ferguson (1994) *e*-cash system comprises of $k + 1$ signatures, where one signature is used for appending the identity of the payor for prevention of double spending and the others are used for designating the value of the *e*-check. Both versions of the Lui et al. (2004) *e*-checks are deemed to be practical protocols for implementation.

Efficient Online Electronic Checks (2005)

In his version of online electronic checks, Chen (2005) claimed that the two electronic check schemes proposed by Chaum et al. (1990a, b) are inefficient. He qualified his assessment of inefficiency based on the need to first decide both the face value of the check and the identification of the payee before check issuance by the bank. The improvement proposed by Chen (2005) opens the possibility for the payor to designate the desired face value of the electronic check as well as the identification of the payee when the check is issued. Chen (2005) attributes the efficiency of his improvement on two grounds: guards against forgery of the information attached and disallows different face values to the same check. The scheme also

boasts of the advantage of simply performing hashing to attach information on the check, which comparatively entails less cost than doing modular exponentiation or inverse computations. The protocol Chen (2005) proposed utilized one-way hash function and RSA signatures, which are both explained at length in Chang et al. (2009).

The scheme proposed by Chen (2005) comprises of three participants: the bank or banking system, the payors, and the payees. The scheme was designed with four phases: *initializing*, *delegating*, *paying*, and *depositing.* Two participants – the bank and the payors are signers and users of digital signature. In the *initializing* phase, bank clients open an account with the bank. In the *delegating* phase, the payor randomly chooses four messages (x_i) which are kept secret, and computes a one-way hash function, **H** for every different x_i and payor then sends the messages to the bank. Upon receipt of the message, the bank computes for the digital signature and sends the same to the payor. The result of the procedure is an e-check, which can be verified using the signature. In the *paying* phase, the payor decides the face value of the check and the payee account number, computes for four one-way hash functions β_1, β_2, β_3, and β_4, and sends the e-check with the designated face value. Finally, in the *depositing* phase, the payee sends the e-check with the 7-*tuple* for verification from the bank database in case of double spending. A *tuple* refers to a set of unnamed and ordered comma-separated values, which may comprise of different types and are used for the creation of ad hoc data structures as a convenient method of returning multiple value (Terrell, 2018). When the 7-*tuple* is absent in the database, the *e*-checking transaction proceeds, where the face value amount of the check is added to the payee account and the corresponding amount is deducted in the payor account.

Online Electronic Check with Mutual Authentication (2009)

Ever since the banking sector and concerned legislators recognized the importance of electronic checking in the financial system, the *e*-check became an indispensable component of electronic commerce. Since the dawn of the new millennium, programmers and banking experts endeavored to implement improvements to boost both the functionality and the security of electronic checking, primarily by way of predetermining the face value of a check and the identification of the payee. However, even with the improvements, the checking system suffers from inflexibility. Chang et al. (2009) recommended an innovative *e*-checking mechanism, which can permit the payer to assign both the face value of a check issued and the relevant information of the payee Security of the proposed system is implemented using a number of cryptographic techniques, particularly *blind signature*, RSA *cryptosystems*, and the *secure one-way hash function*.

The basic concept of an electronic check was advanced in 1988 by Chaum, but the system entails tremendous computation overheads. In the following year, Chaum devised an offline method, but the system neither allows the payor to designate the face value of the check nor the payee identification. The issues in Chaum's design are addressed in Chang et al. (2009), and at the same time, but also offers mutual authentication along with the following features: *mutual authentication*, where verification by the payee of the payor and authentication of the payee by the payor are both possible to bolster the security of the system; *non-repudiation*, where a payer cannot deny an *e*-check issued for a transaction with the payee; *robustness*, where only a legal payor and the trusted bank can jointly coordinate for the purpose of issuing an *e*-check, and the feature provides for the confirmation of the face value of the check to guard

against forgery by fraudsters; and *uniqueness*, where the e-check should be assigned the payor identity to enable verification by the trusted bank.

RSA cryptosystems. A cryptosystem refers to a "system which converts text to cipher text or cipher text to plain text by the application of encryption or decryption algorithm … [where] the key generation for encryption or decryption algorithm is also part of a cryptosystem" (Javid, 2018, p. 53). Cryptosystems are categorized either as symmetric or asymmetric key, where the latter comprise of six components namely: plain text, public key, private key, encryption method, cipher text, and decryption method. In the era of the Internet, security entails a primary issue in secret information transmission between sender and receiver. RSA cryptosystem is regarded as the most popular asymmetric key cryptosystem, which is mainly utilized for key exchange, transmission of secret message, and generation of digital signatures. RSA stands for (Ron) Rivest– (Adi) Shamir– (Leonard) Adleman, who proposed the method for asymmetric public key encryption in 1977. The algorithm uses information blocks and keys of different sizes and implements asymmetric keys for both encryption and decryption. The RSA algorithm generates public and private keys using two prime numbers. To date, it is applied in software products primarily to maintain information security and authentication in an open communication channel (Shaheen & Siddiqui, 2020).

In the Chang et al. (2009) design of an online checking system, the RSA algorithm was utilized for digital signing or in "encrypting with the private key and decrypting with the matching public key" (Thorsteinson & Ganesh, 2004, p.137). In digital signing, encryption of the full original message is not anymore required, but rather, it is practically more efficient that the hash of the general message is encrypted and just to encrypt the smaller hash value with the private key. Given that it is tremendously difficult to get two inputs which can generate the same

hash output, it follows that anyone with the public key that matches the public key during verification can decrypt the hash (Thorsteinson & Ganesh, 2004, p.137).

Secure E-check Payment Model Based on Elliptic Curve Cryptography (2010)

Rui (2010) presented a new pattern for an electronic check facilitated by elliptic curve cryptography (ECC) based on authentication, digital signature, and public key cryptosystem technology. In addition to the typical checking account, the protocol introduced in the Rui (2010) secure e-check payment model provides high-quality security and efficiency. The model is capable of resisting various forms of attack, but relies on a lesser burden of computations and offers better transaction efficiency online.

Given that RSA is the pioneering technology used in Chaum et al. (1990a, b), and is, therefore, comparatively older, some of its limitations have been observed, such as high energy utilization, low computational power, lower process efficiency, poor key generation, etc. which renders it less useful for mobile applications (Paul & Sharna, 2021). Note that at the time of the Rui (2010) study, mobile banking platforms began to emerge as enablers of access to financial services, including balance information, bill payments, investment options, transfer, etc. (BBVA Innovation Center, 2012).

To address the limitations, elliptical curve cryptography (ECC), a public key encryption technique was introduced with the goal of creating more effective, fast and small cryptographic keys based on the equation of the elliptic curve. The technique is described to provide an enhanced security level using 164-bit size key compared to RSA which implements 1024 bit-size keys. The ECC is also much better than the hash function because whether the hash function is asymmetric or symmetric and whatever the size of the message, encryption is slow. The cost of

implementing hash function for optimal security also entails more expense for hardware, licensing, and maximum overhead in addition to issues related to correctness and impersonation (Paul & Sharna, 2021).

The protocol for a secure *e*-check proposed by Rui (2010) consists of three phases: *application*, *issuing*, and *verification*:

Verification. In the application phase of the e-check in Figure 3, the user (i.e., the payor) computes the application information, including the payor account, time of application, serial number and validity and signs the application information using the elliptical curve signature algorithm to generate the digital signature, Sa. The connection (||) of the e-check application information and the digital signature is place as the digital envelop (APu). The user then performs encryption of the digital envelop by way of the session key (Ksab) and sends it to the bank. The symbols D, E, and H, represents decryption, encryption, and hash function, respectively.

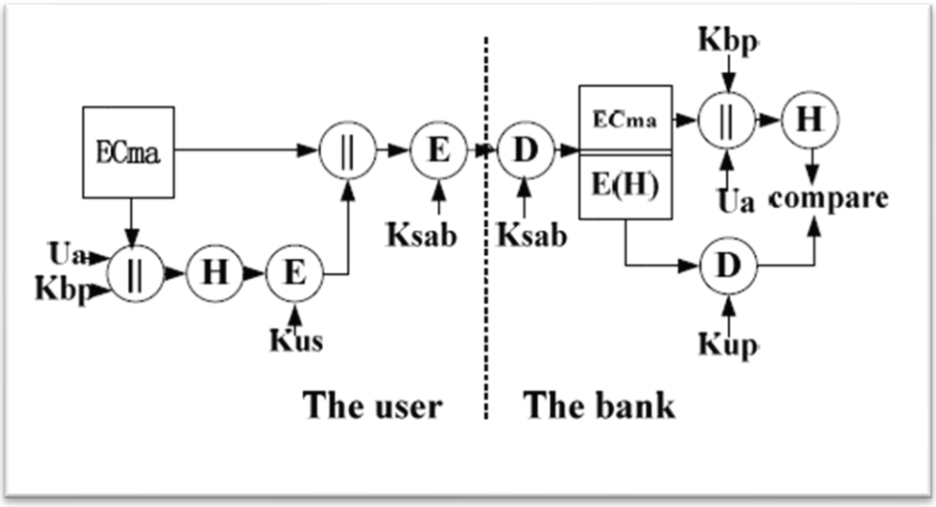

Figure 3. Application and verification of the *e*-check (Rui, 2010, p. 110).

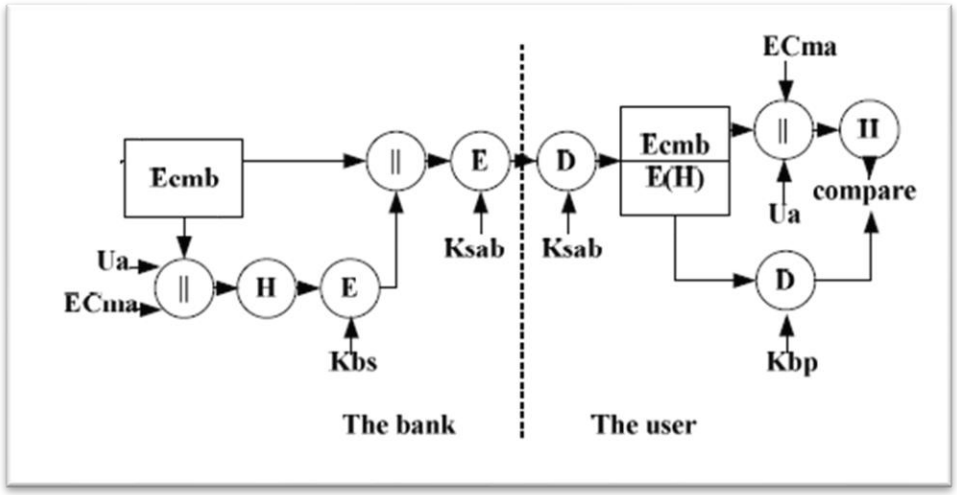

Figure 4. Issuing and verification of the *e*-check (Rui, 2010, p. 111).

Issuing. Figure 4 shows the steps in the issuing phase. Upon receipt of the encrypted application by the bank, Ksab(APu) undergoes decryption using the session key KSab to obtain the application information of the *e*-check and performs authentication of the digital signature for confirmation of user legitimacy. A successful verification results in the issuance of the *e*-check ECmb containing the issuing bank, issuing time, maximum amount, serial number, etc., and computes the *e*-check message digest CB, signs the CB using the bank private key (Kbs) to obtain the result (Seb) and the digital envelop of the *e*-check (Bpb). The bank then encrypts Bpb with the session key, send the same to the user, and associates the serial number of the e-check to the user account with the e-checks set to "inactive". The bank permits use of the *e*-check upon receipt of the activate signature from the user.

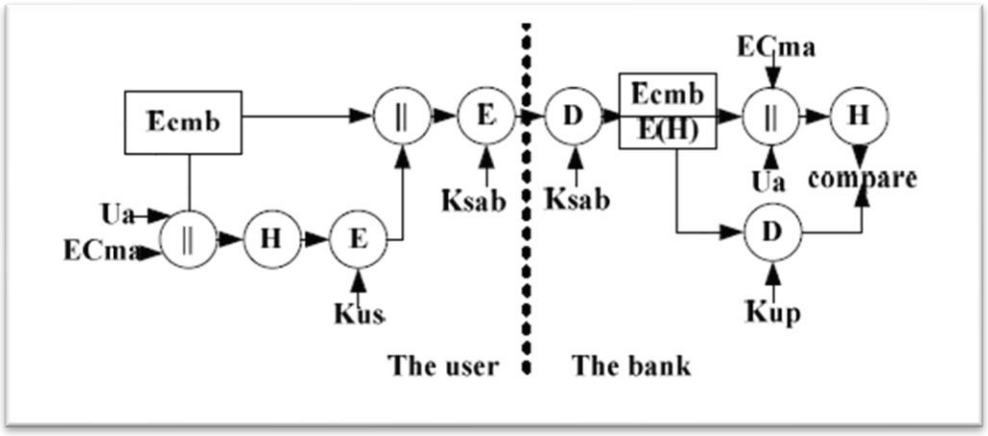

Figure 5. Activation and verification of the *e*-check (Rui, 2010, p. 111).

Activation. Upon receipt of Bpb, the bank verifies and a successful the *e*-check is bank-validated and accepted by the user. The user then computes for CU, signs it with the private key (Kus) and obtains the digital signature (Subs). The user encrypts the digital signature associated with the account information (Subs||ECmb) by way of the session key Ksab and sends the encrypted message to the bank for the activation of the *e*-check. A successful verification of the *e*-check activates it for use in a payment transaction.

Security of the ECC-facilitated *e*-check system in Rui (2010) is ensured under the framework of the Secure Electronic Transaction (SET) protocol to satisfy the requirements of authentication, confidentiality, integrity, non-repudiation, security etc. The secure *e*-check system also bolsters the diversity in secure electronic commerce transactions (Rui, 2010).

Fraudulent Electronic Transaction Detection Using Dynamic KDA Model (2015)

With the coming of age of an information-conscious society, data mining, or the process of extraction of potentially useful information from raw data to discover useful patterns from the massive volumes of data. In e-commerce and financial services, mining techniques and algorithms have found significant application for protection of security of information (Sravanthi & Rao, 2017. Vadoodparast et al. (2015) ventured to secure the information security of banking

services based on actual bank-provided data using clustering analysis and data mining techniques, such as the KDA model, which represents the three clustering algorithms: K-means, DBSCAN, and agglomerative.

Clustering analysis comprises a common method in data mining and is performed by grouping related data points in a network with the goal of revealing unusual patterns for fraud or anomaly detection. The technique may also be utilized in a new database without the benefit of pre-determined data categories (Bu, 2018). Meanwhile, K-means refers to a well-known hard clustering technique performed by partitioning a dataset for analysis into disjoint clusters to obtain continuous data (Lakshmi et al., 2019). To cover for the limitation of K-means clustering, the DBSCAN algorithm, which is the acronym for Density-Based Spatial Clustering of Application with Noise, was also used in Vadoodparast et al. (2015). DBSCAN is capable of detecting randomly-shaped and sized clusters, but requires input of two parameters, which is a crucial process for the algorithm to generate results as expected. In other words, DBSCAN refers to a density-based algorithm which automatically groups data into sub-classes (Starczewski & Cader, 2020). On the other hand, agglomerative or hierarchical clustering generates tree-like clusters, which data miners or researchers can investigate after clustering. This form of clustering algorithm does not assign a single cluster to data points. The clusters gradually merge to form larger clusters until all records in the database are in one large cluster, unless, cluster merging is stopped at a certain point in the data analysis (Linoff & Berry, 2011).

The Vadoodparast et al. (2015) utilized a set of data mining clustering analytical techniques in proposing a dynamic model and mechanism to bolster the limitation of a specific bank's fraud detection system (FDS). Hence, the strengths and limitations of the three clustering

techniques were considered to optimize the efficiency of the FDS. The KDA model implemented in the study is schematically illustrated in Figure 6.

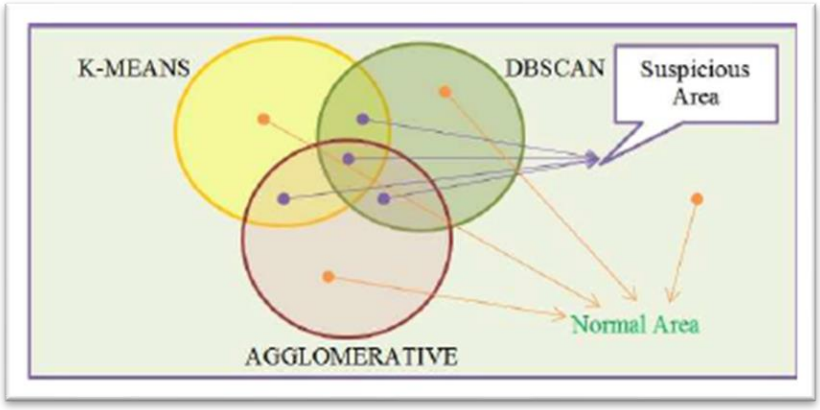

Figure 6. Schematic diagram of the KDA model implemented in Vadoodparast et al. (2015, p. 93).

In Figure 6, the diagram of the KDA model, for each transaction in the network database, each record of the transaction has three labels for the detection of abnormality, where each of the three algorithms may use some or all parameters of the dataset. Suspicious transactions in th minimum members cluster in K-means, high LOF values in DBSCAN and in single-mode form in the agglomerative technique. Fraudulent transaction is suspected when a new transaction is detected by two or more algorithms and these transaction(s) occur in the suspicious area (Vadoodparast et al., 2015). Figure 7 shows the proposed FRS by Vadoodparast et al. (2015).

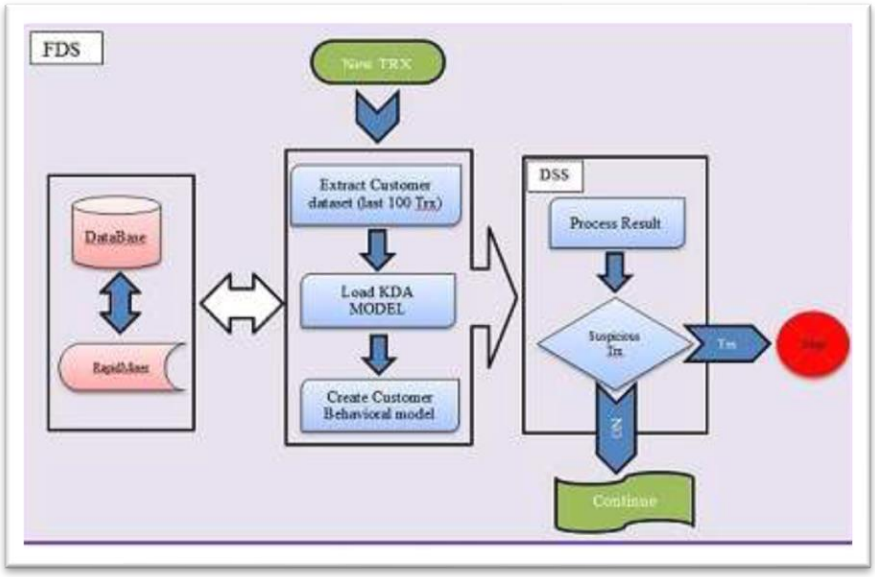

Figure 7. The proposed flow of the fraud detection system proposed by Vadoodparast et al. (2015, p.95)

In the FDS proposed in Vadoodparast et al. (2015) depicted in Figure 7, the system driven by the KDA model inspects the suspicious area. In the event of a transaction which takes place in the suspicious area, the proposed system will trigger an alert and advice the bank client to inspect/verify the transaction or otherwise stop it.

Fraud Track on Secure Electronic Check System (2018)

With the burgeoning growth of the Internet and mobile banking and other financial services, particularly in the e-checking system, security consistently figures among the key concerns, along with the concomitant issues of confidentiality and privacy, as well as the ease with which electronic documents can be perfectly duplicated like the original, or worst, counterfeited. Hence, fraud detection remains a critical goal in the continuous development of the digital checking system. The Zhang et al. (2018) work proposed a method of implementing a secure *e*-check system, which can defend against most of the most fraud schemes and analyzed how *e*-check fraud can be traced using a forensic perspective. Among the solutions employed are digital

signatures and out-of-band transaction verification, where the former guarantees authentication, integrity of information, and non-repudiation, whereas the latter protects the system from MitB attack. Figure 8 presents the proposed flow of the *e*-check to protect it against MitB attack.

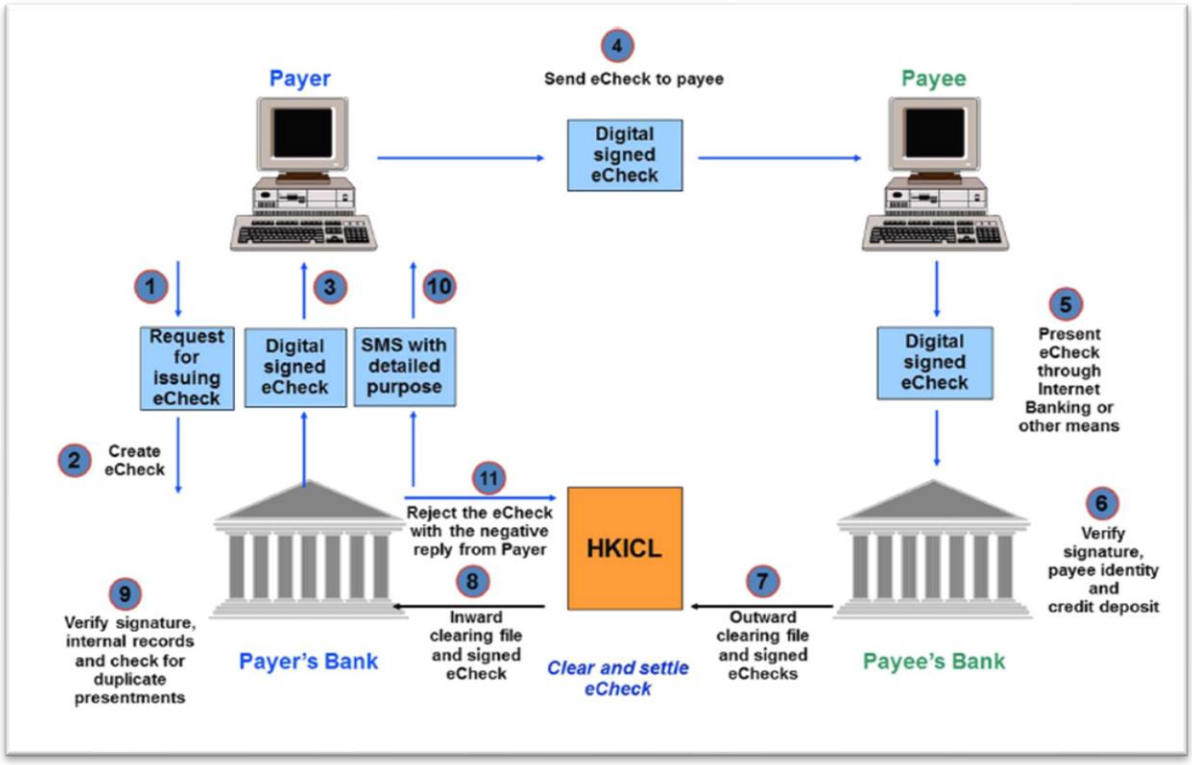

Figure 8. Flow of e-check to defend against MitB attack (Zhang et al., 2018, p. 143).

As illustrated in Figure 8, to defend the bank network from MitB attack, an additional authentication factor can be implemented along a channel other than the browser in use. This facilitates confirmation if the *e*-check pays for its initial intended purpose. The problem, however, with a simple confirmation code, such as an SMS, is that this may not hold out against a MitB attack given that the attacker may be able to modify the browser content in his favor. The vulnerability of the link for a simple authentication code may be solved using an out-of-band transaction verification, which utilizes an authentication channel between payor and payee without using the compromised browser. This will enable the payor to obtain a description of the

purchase and suspicious or inconsistent details can hint the payor of a possible fraud (Zhang et al., 2018).

A Privacy Enhanced Transferable Electronic Checkbook Scheme (2021)

The proposed Sertkaya and Kalkar (2021) scheme for an *e*-checkbook is described to support transferable e-checking and protects user anonymity against cyber-eavesdropping. The researchers introduced their proposed scheme by an operational game-based security definitions that render *e*-checkbook unforgeability, *e*-check unforgeability and non-manipulability, and *e*-check anonymity. Sertkaya and Kalkar (2021) first defined the cryptographic primitives they applied and used the signcryption procedure and justified how the methodology supports unforgeability for both the *e*-checkbook and the *e*-check, non-manipulability, and anonymity, as well as successfully guards against double spending and replay attacks.

A *cryptographic primitive* consists of a pair where the first term is a set of functions and the second term is a relation over a pair of functions and a machine, where the set must include at least a function capable of being computed by a probabilistic polynomial-time (PPT) Turing machine (Reingold et al., 2004). Meanwhile, the *signcryption* algorithm refers to a public key primitive, which simultaneously performs digital signing and encryption to guarantee honesty, non-repudiation, and privacy (Shankar et al., 2019). In the signcryption scheme proposed in Sertkaya and Kalkar (2021), the payor/sender sends an encrypted message to the payee/recipient, such that the message can only be meaningful to the intended recipient and be assured that the message emanated from the payor/sender. To accomplish these twin objectives, signcryption algorithms will be implemented so as to offer end-to-end security and receipt of the intended message is guaranteed even if the recipient is offline at the instance of message sending/delivery. In the proposed *e*-checkbook scheme in Sertkaya and Kalkar (2021), four participants are

recognized: the payor (sender); the payee (receiver); the e-checkbook issuer which carries out the transfer of payments; and the acquirer, where the payee account is maintained. Four phases are identified: issuance, payment, transfer, and deposit. Figure 9 presents the conceptual model of the *e*-checkbook consisting of transferable *e*-checks.

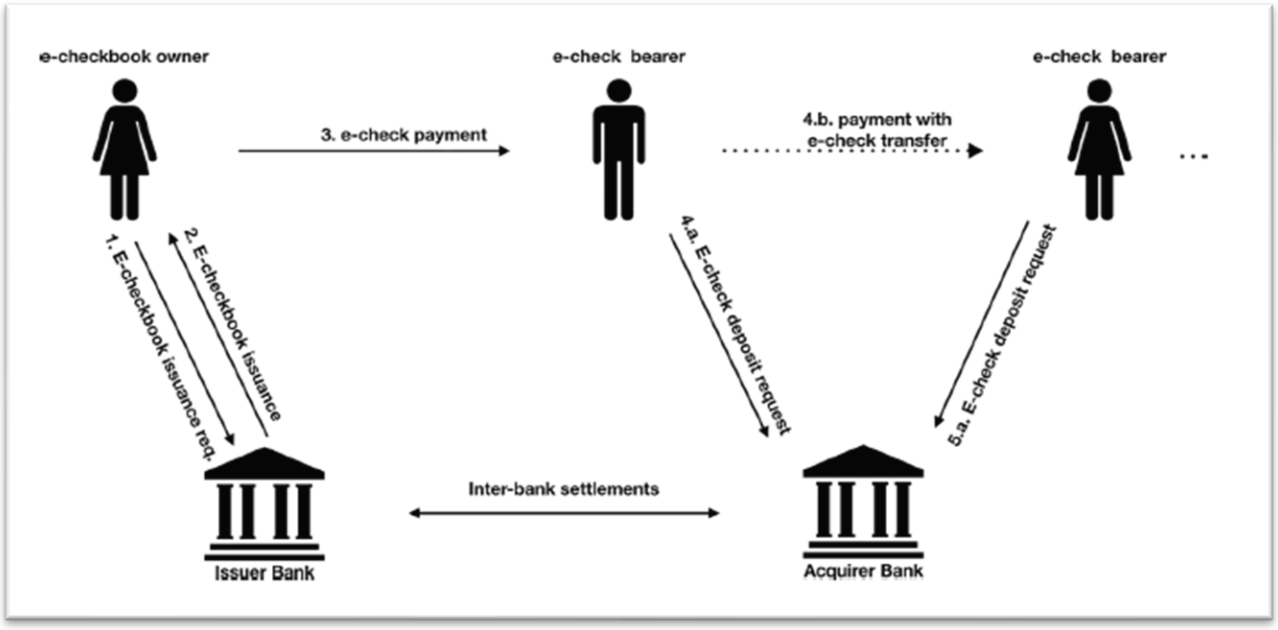

Figure 9. Conceptual model representing an e-checkbook with a transferable check (Sertkaya & Kalkar, 2021, p. 6).

Methodology

The method used to analyze the literature and information presented to address the research questions is the integrative review. Integrative review (IR) implements a broad approach and diverse sampling by including both empirical and theoretical literature (Toronto, 2020). Studies apply IR to empower the analysis in exploring and addressing the present state of research literature concerning a specific phenomenon, assess the quality of the evidence, identify gaps in the literature, and identify the future direction of research and practice (Toronto, 2020). The goals of IR fit the objectives of the capstone project as the first objective explores the evolution of digital checking technology-wise, which can be achieved by evaluating the state of literature since the initiation of digital checking until the present by appraising the quality of the random evidence retrieved from 1989-2021. The second research objective weighs how technology and other factors fueled the development of digital/electronic checking and if the desirable attributes of a payment instrument are present in the *e*-check. This can be accomplished by identifying the gaps in the sampled literature. Finally, in order to recommend possible future directions for research and design implementation of digital checking, IR also serves as a powerful mechanism to sieve through literature and emerging theory.

As recommended in Toronto (2020), an IR is best guided by the use of a theoretical framework discussed and shown below to guide the process, referred to as the basic systems model or the input-process-output (IPO) framework. The IPO framework consists of feeding inputs into a system, where processing or analytic activities take place, with the generation of the result or output completes the process (Anderson & Yull, 2002).

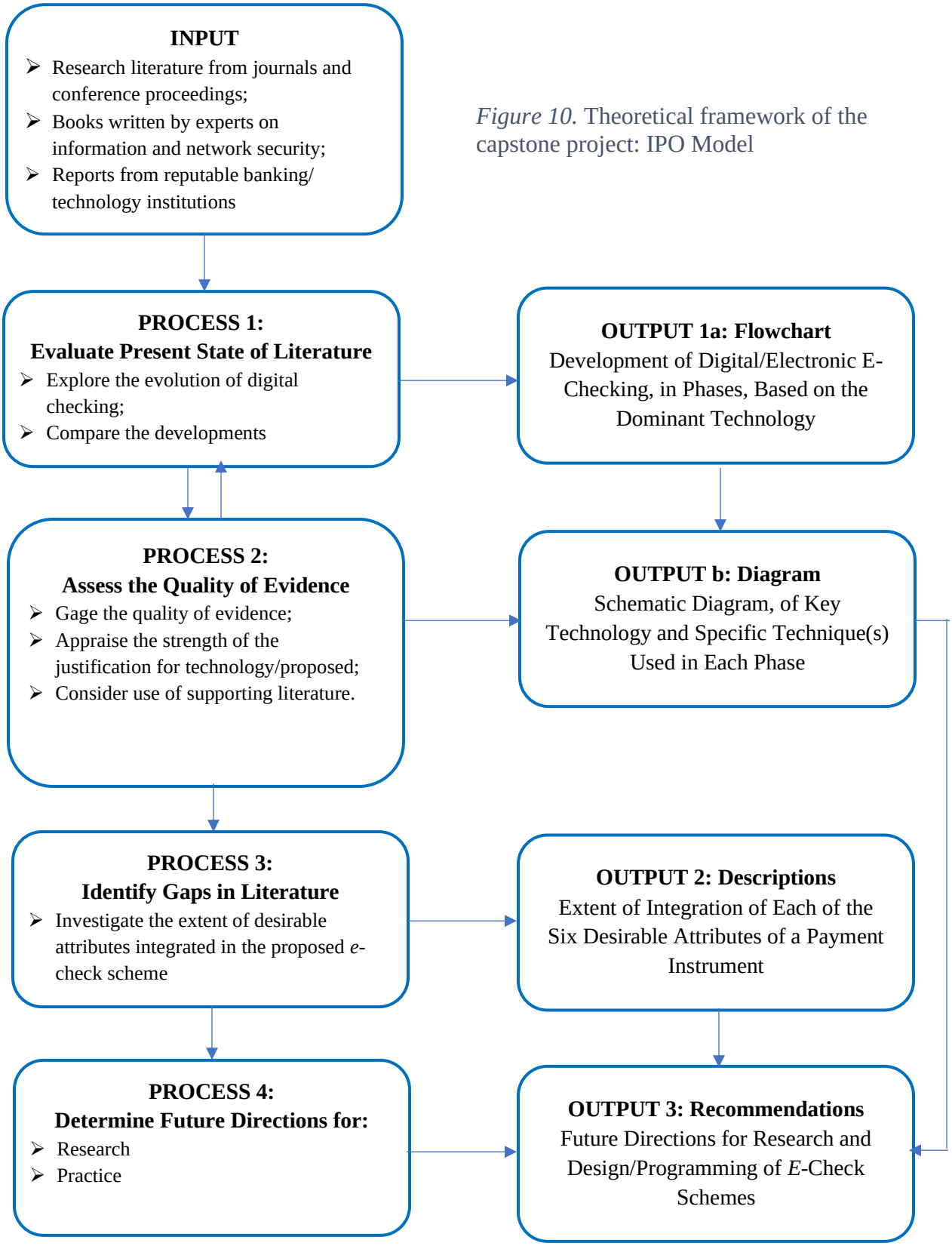

Figure 10. Theoretical framework of the capstone project: IPO Model

Analysis and Results

This section presents and summarizes the findings of the analysis performed to address each of three research questions. Each research question is discussed in a separate subsection, together with the summary presented as part of the project deliverables. Supporting literature from journal research articles and theoretical knowledge from technology resources are provided when necessary.

Research Question 1: How did digital checking evolve technology-wise?

The research literature sampled revealed that since the introduction of the concept of digital/electronic checking in 1989 until 2021, cryptography, at different levels of complexity depending on available technology during the particular timeline, is a popular modality in conceptualizing the various digital checking schemes. The evolution of digital checking in this capstone project may be reasonably divided chronologically in three phases. Phase 1 is the period from 2001 and earlier, whereas the next two phases are each a decade long. Phase 2 is from 2002-2011, and Phase 3 is from 2012-2021. The findings for Research Question 1 are summarized as a flowchart in Figure 11.

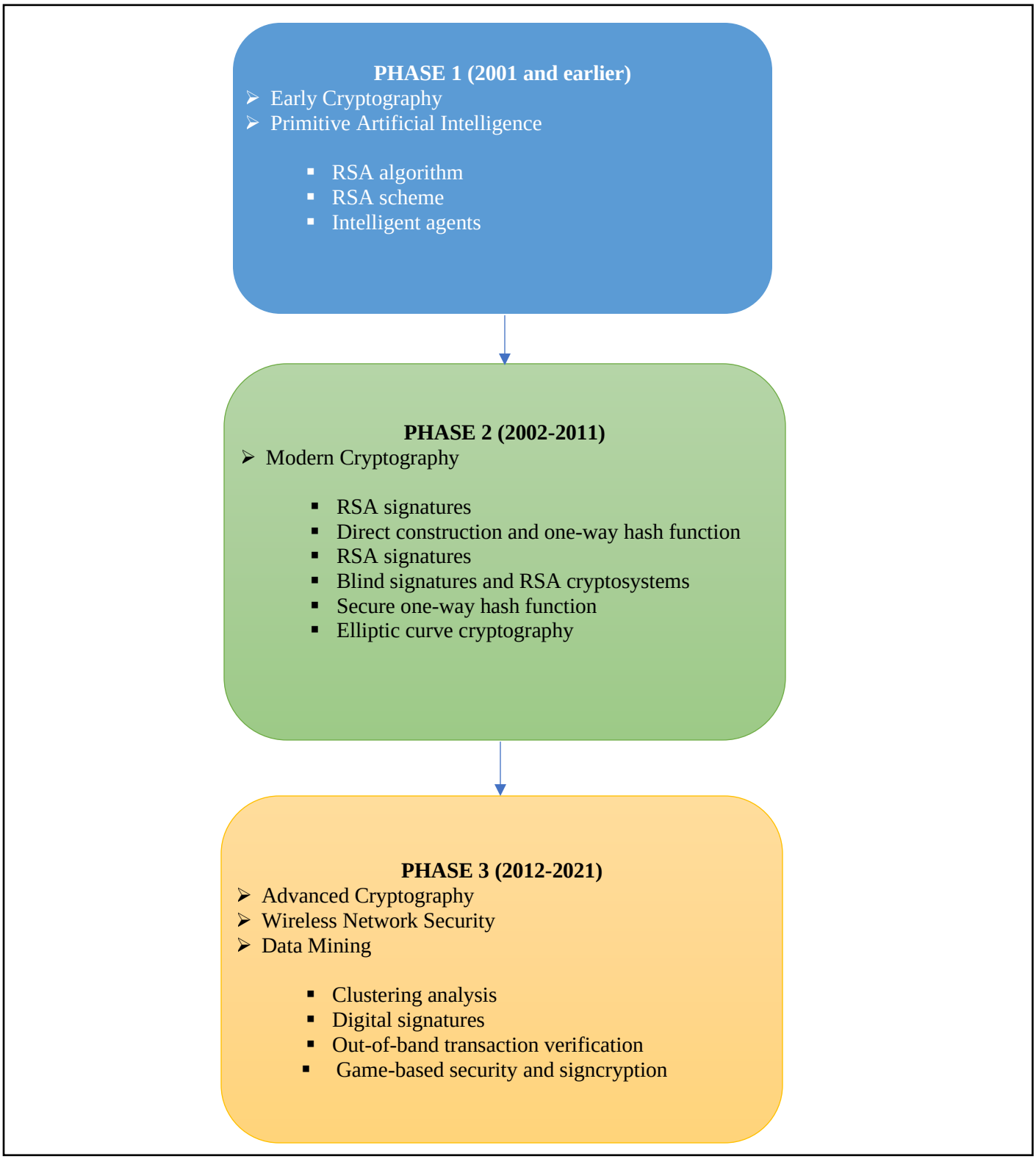

Figure 11. Flowchart of the development of digital checking based on dominant technology and specific techniques

Research Question 2: What factors influenced the development and advances in the digital checking system?

The research articles sampled for the literature review apparently illustrates the role of human ingenuity and motivation for innovation in the development and advancement of the digital/electronic checking system since the concept was proposed in 1988 in Chaum et al. (1990a) up to the previous year (i.e., 2021). In Phase 1 of the evolution of digital checking. Chaum et al. (1990b) admitted that their work in Chaum et al. (1990a) was not perfect and the latter introduced improvements in terms of unlinkability, anonymous withdrawal and simpler calculations and operations. When the new era began, Lee and Yoon (2000) applied innovation to their previous work using primitive artificial intelligence referred to as intelligent agents.

In Phase 2 of the evolution of digital checking, Liu et al. (2004) innovated a decade-old work of Ferguson (1994) by implementing direct construction or the use of polynomials over limited fields, which satisfies the lower bounds of key-sizes with equalities, rather than the cut-and-choice technique. Liu et al.'s (2004) innovation improved on unlinkability of *e*-checking. Similarly, Chen (2005) attempted to enhance the *e*-check having evaluated the Chaum et al. (1990 a, b) schemes as inefficient given the unlikability need to first decide both the face value of the check and the identification of the payee before check issuance by the bank. Chang et al. (2009) also proposed an online checking system to simplify the complexity of computations required in Chaum et al. (1990a) and the benefits of mutual authentication, non-repudiation, robustness, and uniqueness using blind signature and RSA cryptosystems. Rui (2010) also enhanced the pioneering works of Chaum (1990 a, b), implementing emerging technology as programmers achieve familiarity with such new techniques as elliptical curve cryptography

(ECC) for the design of more effective protocols using fast and small cryptographic keys based on ECC).

On the other hand, design and development of Phase 3 schemes for digital/electronic checking benefited from the surge of newer technology not just in the field of cryptography, but in wireless network security and data mining, as well. Vadoodparast et al. (2015) designed a new scheme for more secure banking services by adopting the strengths of clustering analysis in data mining, but neutralizing perceived limitations by using a hybrid of K-means, DBSCAN, and agglomerative clustering methods. Zhang et al. (2018) implemented a combination of early and newer cryptographic techniques and applied them to their proposed fraud tracking scheme for improved security. Finally, the protocol proposed by Sertkaya and Kalkar (2021) was also motivated by innovation as they assessed correctness, e-check anonymity, mutual authentication, and transferability of six relevant schemes as to features and security. Their proposed e-checking design applied the newer technologies of game-based security from wireless communications and signcryption, a more novel algorithm in advanced cryptography.

According to the report of Auer et al. (2020), from the management and operations perspective, the drivers of advancement and growth of the e-checking system have also been fueled by: (1) digital infrastructure, where adoption of digital checking is catalyzed by the penetration rate of the Internet, as well as the rate of mobile phone usage among the relevant population; (2) innovation capacity of a country or region, which in turn is dependent on the availability of enabling infrastructure; business sophistication of the financial and commercial sectors; educational level of banking clients; and the political environment; (3) institutional quality, which pertains to higher government effectiveness and interest in creation of data trail for transactions; (4) development and financial inclusion, which involves the extent of financial

development; and (5) cross-border transactions, which particularly refer to a country or region's openness to trade and flow of remittances.

Therefore, with respect to both the users and providers of digital/electronic checking, the development and advances in e-checking evaluated via the extent of integration of the six attributes of a payment instrument, summarized in Figure 12, based on the literature review and supporting resources. The extent of integration of the six desirable attributes of e-checking as a payment instrument was evaluated based on an arbitrary scale showed as Appendix 1. The scale in Appendix 1 was created based on the capstone literature and additional support resources, which are indicated in the scale under each desirability attribute. The extent descriptors – very high, high, medium, and low – were identified for each of the attributes.

As illustrated in Figure 12, the main issue of e-checking as a payment instrument is security, garnering an extent of desirability on a medium level. As shown in Appendix 1, a *medium* extent is used to indicate that present security threats are being neutralized as depicted in the capstone literature, but newer threats are evolving fast. Among others, Chen (2005) and Chang et al. (2009) worked to boost the security of earlier online (*e*-checking) systems. However, not only network security professionals harness the benefits from advancing technology, but fraudsters and scammers, as well.

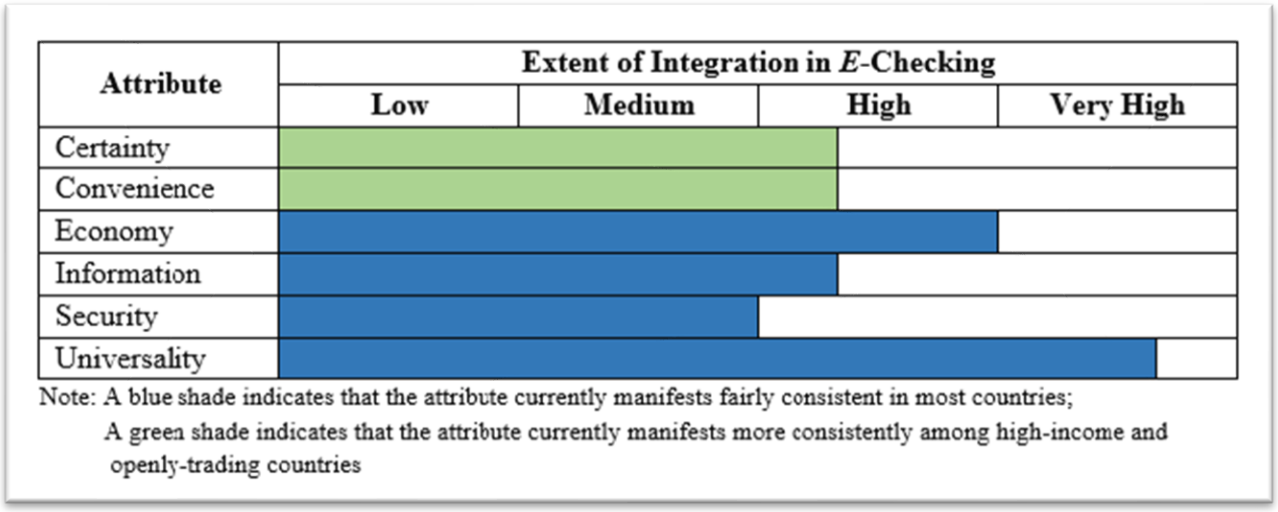

Figure 12. Extent of integration of the 6 desirable attributes of a payment instrument in e-checking

In about five or six years, new security threats evolved as documented in the capstone literature by Vadoodparast et al. (2015) who adopted more advanced technology through clustering analysis and data mining. Nevertheless, Zhang et al. (2018) found the need for more robust security protocols using the emerging cryptogfraphic techniques to address the security threats only three years after the enhancements in Vadoodparast et al. (2015). To be clear, the studies cited in the capstone literature are not the only research which addressed network security and wireless communications. Other support resources include Guo et al. (2018) and Chiou et al. (2019), where the former applied smart cards to check network security threats, and later found out that smart cards are vulnerable to online guessing attacks. Sertkaya and Kalkar (2021) further assisted in the improvement of *e*-checking by protecting against cyber-eavesdropping using *sign-cryption* technology as a cryptographic protocol. Hence, the capstone literature and support resources showed that security threats are being naturalized as these are perceived, but newer threats evolved fast with the influx of more sophisticated technology. As such the security aspect of *e*-checks as a payment system is on *medium* level.

The desirability of a payment instrument attribute of *universality* pertinent to online or electronic checking was evaluated from literature to be *very high* although not perfectly very high, but about midway the high to very high scale. It is believed to be globally accepted by all payment institutions, payers and payors (Jacob et al., 2009). In 2000, the volume of *e*-check payments was 5.6 billion, amounting to USD 5.7 trillion (Gerdes & Walton, 2002). After two decades, the volume of *e*-check payments was 26.8 billion, amounting to USD 61.9 trillion (National Automated Clearing House Association [NACHA] 2021). These figures manifest universality of acceptance of online electronic checks. However, the extent was not solidly very high because there is no official governing standard for *e*-checks. Rather each country has its own national electronic check clearinghouse, such as the ACH for the US and the Single Euro Payments Area (SEPA) in Europe (Rampton, 2022). Hence, the legal infrastructure for a global standard is not yet in place.

Meanwhile, as shown in Figure 12, economy as a desirable attribute of online or electronic checking was evaluated to be on its full scale on the *high* level due to its acceptable and reasonable transaction costs of maintenance and operation (Jacob et al., 2009). Electronic checks, as a service provided by practically all banks nowadays, and also called Automated Clearing House (ACH) processing, charger lower transaction costs than with credit cards or even debit cards (Belew & Elad, 2017; Blaney, 2020). Although banks have a range of fees to cover electronic or online checking services some charge from $0.30 to more than a dollar (Belew & Elad, 2017). Comparatively, the median transaction costs are $0.26 – 0.50 for e-checks, vs. $1.50 or more for debit and credit cards (Blaney, 2020).

Three other attributes were assessed to be a least midway through the *high* level: convenience, certainty, and information. The attribute, *information*, of a desirable payment

system entails 4 sub-attributes: specific user knowledge and familiarity in processing/recording transactions; ease of recognition of payee identification; infallibility of authentication; and availability of information sources (Jacob et al., 2009). For online or electronic checking, almost all user-types (i.e., individual payor, and payee, merchants, and bankers) have average or above average familiarity, and for banks – there is perceptible reliability of payee identification and authentication, as well as abundance of information sources provided for all user types. There is considerable familiarity among all user types because e-check technology has been around for over half a century. The ACH network and comparable networks in other countries have consistently modernized infrastructures and policy to keep up with the industry demands. Recently, the updates to *e*-checking service includes shorter transfer period for larger amounts to facilitate same day transaction processing (Mondonedo, 2020).

However, certainty and convenience appear to be enjoyed better mostly by clients of e-checking facilities in high-income countries and those that engaged more in open trading. Thus, the green shading as explained in Figure 12. While most banks globally can process *e*-checks within 24 to 48 hours, the absence of a standard legal framework applicable to all countries is not yet in place (Mills, 2019; Rampton, 2022). Hence, there are still differences in processing times, transaction costs and transferable amount across countries, but the certainty attribute is on a *high* level. Likewise, convenience as a payment instrument is also high for *e*-checks on account of its non-arduous processing for both initiation and receipt (Bidgoli, 2020; Carnell et al., 2021), but the benefit of convenience is mostly limited to high-income and open-trade countries, especially those with higher ranks in ease of doing business. Implementing payments through online checking bolsters the workflow of accounts payable (Ghassemian, 2017).

Research Question 3: In what direction is the future of digital checking technology headed in terms of addressing emerging technology-enabled security threats?

In as much as the capstone project pertains to a technical subject matter, the most relevant gap noted from the literature review that needs to be addressed are those which pertain to security threats, wherein security is one of the six desirable attributes of a payment instrument. However, security provision may be able to ease some of the gaps in certainty and convenience to ensure that all countries attain a comparable level of desirability regarding these attributes

It may be noted in Phase 3 that all three sampled literature – Vadoodparast et al. (2015), Zhang et al. (2018), and Sertkaya and Kalkar (2021) – all tackled security threats, particularly fraud. Hence, the gap in literature about the need for more efficient security protocols needs to be addressed. Fraud in different forms is the key security issue tackled in all the sampled literature in Phase 3 of the evolution and development of digital/electronic checking. According to the literature, promising and emerging modalities for the identification of authentic participants in a banking/financial services network include the following technologies:

Biometrics. Biometrics integrated with the Internet of Things (IoT) presents a novel modality applicable to wireless security. Biometrics embedded in the IoT of banking/financial services institutional facilities offers an avenue for network integration, privacy, and availability. Biometrics is trustworthy authentication of user identity for various transactions.

Goode (2018) observed that even banks all over the world are turning to biometric technology for client identification and authentication, protection of high value transactions, and in combating fraud. He further claimed that “the latest digital platforms, this technology is

proving to be the sole reliable means to authenticate and secure banking customers across all channels" (Goode, 2018, p. 5). However, every technology has inherent risks, questions and implications to privacy protection and other legal and moral aspects served as barriers to a higher adoption rate of biometrics for security protection (Whiskerd et al., 2018). In this respect, it would be a more viable direction for better fraud protection to abide by universal human rights guidelines, such as those of the United Nations, and consider deidentification approaches for soft biometrics of the face and fingerprints were suggested in Whiskerd et al. (2018).

Quantum cryptography. While the RSA algorithm, which was used extensively in Phase 1 and Phase 2 periods of the evolution and development of digital checking, may be regarded as an outdated technique by any measure, cryptography too, is evolving as new technology becomes available.

To date, quantum cryptography or quantum key distribution (QKD), powers unbreakable encryption and the perceived risks are only hypothetical (Denning, 2019). QKD is the first commercial application of the principles of quantum information, where an eavesdropper on a (wireless) network who gains entry will be revealed. QKD also limits the any leaked information to a maximum "harmless" and useless amount. This is made possible through the use of a fiber channel or a free space connection which transmits feeble light signals (Weinfurter, 2014).

However, quantum cryptography may still present risks in the future, and it will require substantial technical advances before technophiles can succeed the strong code now in current, but limited use (Denning, 2019). Nevertheless, Denning (2019) warned readers to be cautious about Internet communications and financial transactions being victimized by quantum attack. Hence, another possible future direction of protecting security threats to *e*-checking and related banking transaction using quantum cryptography/QKD will be to analyze and investigate

through research and simulation about the possible pitfalls of digital cryptography to be a step ahead in fraud prevention.

Blending of data mining and artificial intelligence techniques. With the emergence of big data and data mining, machine learning made a crossover from artificial intelligence to fortify the emergence of data science. Besides, database segmentation, deviation detection, link analysis and predictive modeling, data mining offers a powerful ground for information security protection via machine learning techniques (He & He, 2020). The overlap of machine learning across data science and artificial intelligence presents its as a viable future direction for protection against security threats, particularly through neural networks and deep learning. *E*-commerce flourished in the emergence of an information society and as the vast information collected so far served as the motivation for big data (Sarker et al., 2020).

The efficiency of security protection in wireless networks rest on multiple layers of authentication. In this respect, deep learning, which powers both data science and artificial intelligence, performs even more efficiently as the volume of security data increases. As explained in Sarker et al. (2020), the mechanism of deep learning is similar with the human brain in the interpretation of large volumes of data. It can be recalled from the literature review that a hybrid of clustering analysis techniques documented in Vadoodparast et al. (2015) proved to be efficient in fraud protection more than half a decade ago. Clustering analysis is a mode of unsupervised learning. Therefore, the future direction of protection against security threats may be focused on deep learning because model building requires less effort as well as the advantage of a shorter test time, although training the algorithm may take longer.

Conclusions

In the light of the research articles sampled in the Literature Review and the analysis of the findings, the following conclusions are drawn for this capstone project:

1. The evolution of digital checking since it was theoretically proposed by Chaum et al. (1990a) in 1988 and its first use a decade later was dominated by cryptography in its early, modern, and advanced forms. This suggests that **the future of digital-checking**, particularly in terms of protection of security-related threats, **could also benefit from emerging advances in cryptographic techniques**.
2. The role of **human ingenuity and motivation for innovation figured most in the development and advancement of the digital/electronic checking system, facilitated by the flow of technology**. However, the *e*-checking system evolved also as a consequence of changes in operations management of financial services, based on such factors as digital infrastructure, innovation capacity, institutional quality, development and financial inclusion, and cross-border transactions. All these influences may be harmonized into the six desirable attributes of e-checking and most other payment instruments: certainty, convenience, economy, information, and security.
3. The key gap observed from the sampled literature pertaining to the wider adoption of *e*-checking globally is addressing emerging security-enabled threats. Hence, the future of digital checking technology hinges on research and subsequent practice and implementation of emerging modalities including biometrics, quantum cryptology, and a blending of data mining and artificial intelligence, such as deep machine learning. **The success and wider adoption of e-checking as a payment instrument for e-commerce transactions, however, relies on the observance of the implications of legal aspects**

and human rights in the implementation of technological solutions to security threats.

4. Drawing on the findings and analysis of 10 online checking process research, Figure 13 concludes this study with the recommended process flow of an ideal online checking system, integrating new and emerging technology to prevent cyberattacks, particularly a futuristic quantum attack.

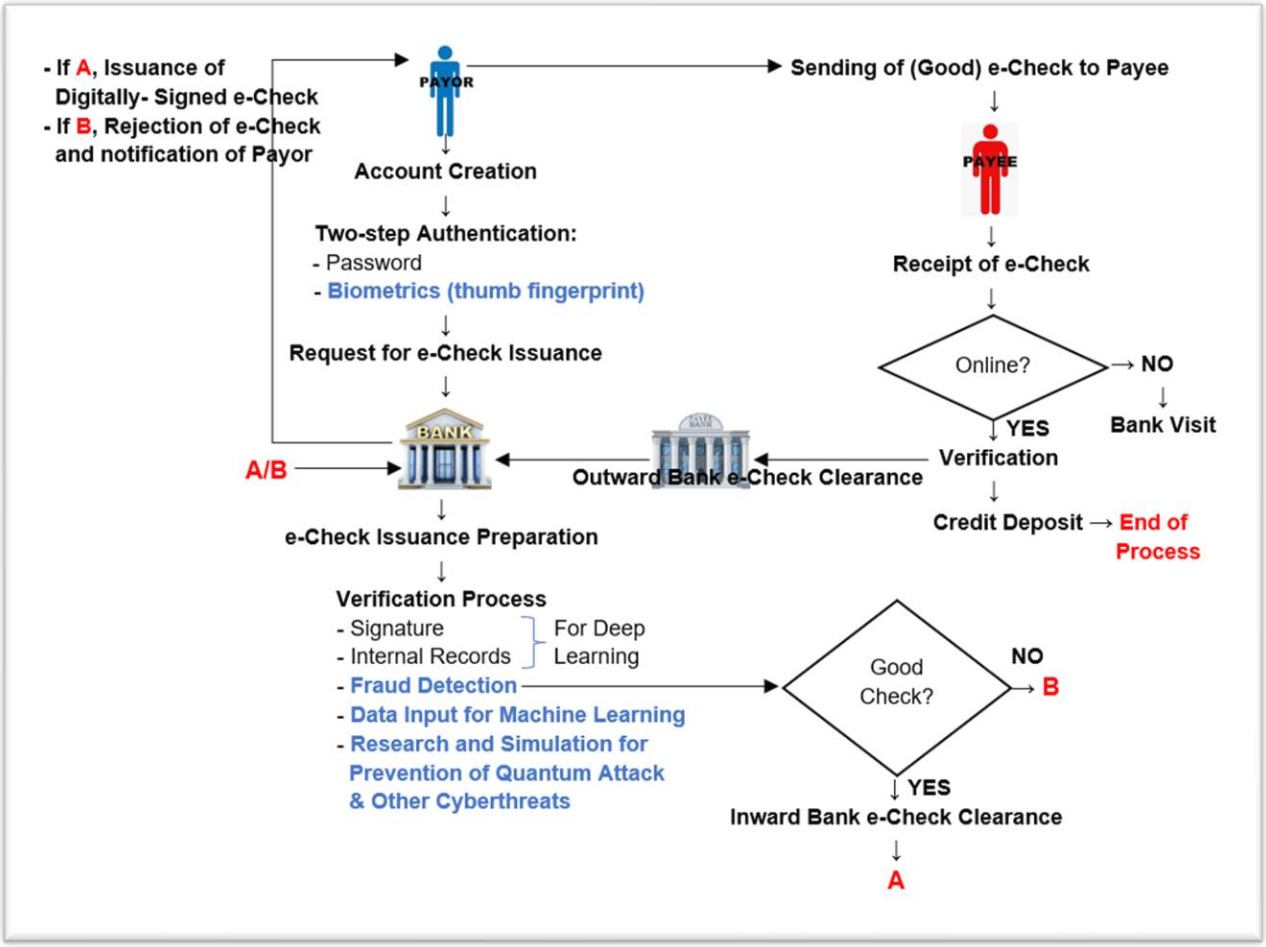

Figure 13. Recommended process flow for a single transaction of an ideal online checking system of today and the near future

In Figure 13, the images (payor, payee, the check issuing bank of the payor, and the check destination where the account of the payee is held) are the main participants in the recommended online checking, which were adopted from all the ten articles sampled in the literature review of

this capstone project. Meanwhile all processes in **black** font, such as account creation, authentication, e-check preparation & issuance, verification, inward back e-check clearance, outward bank e-check clearance, issuance or rejection of e-check, sending of e-check to payee, receipt and verification of the e-check are the best points adopted from the literature sampled. The texts in **red** font are either connectors or milestones in the process flow to ensure a smooth path for the recommended e-checking system. Additionally, the processes in **blue** font are recommended enhancements from a hybrid of the best elements of the sampled literature and the recommended techniques from Research Question 3 indicating the direction of an ideal online checking system for today and the near future. The recommended techniques point towards digital checking technology capable of addressing emerging technology-enabled security threats.

Recommended Enhancements

1. ***Biometrics***. The authentication process is a typical element of an online checking system, which is generally accomplished through passwords. In the recommended process flow a two-step authentication is used: first, with the password, and second is biometric technology using the thumb (finger) print. Biometrics offer a secure second step in the authentication process because like the human genome, no two fingerprints from two different people are exactly alike (Dennett, 2014).
2. ***Fraud detection using quantum cryptography*.** As part of the verification process, a more secure, stable, a robust fraud detection system is "unbreakable" at present and in the near future (Denning, 2019). The technology also reveals any cyber-eavesdropper who gains entry into the fraud detection system (Weinfurter, 2014).
3. ***Data input for machine learning and application of deep learning***. Deep learning models can be used to process large volumes of data through a number of techniques,

such as convolutional neural network, long-short term memory network, multilayer perceptron, and recurrent neural network, can be harnesses to fortify the cybersecurity of web-based systems. (Sarker et al., 2020).

4. ***Research and simulation for the prevention of quantum attacks and other emerging cyberthreats via a blend of data mining and more highly-advanced artificial intelligence.*** The only way for cybersecurity experts to be one- or two-steps ahead of online network fraudsters and scammers is to proactively detect threats and find solutions before the unscrupulous tech can find possible network hacks. As early as now, online checking programming and cybersecurity experts should collaborate to continuously collect data, and simulate data breach attacks to address any emerging security threats. A blend of data mining and artificial intelligence may be applied to fortify the vaunted "unbreakable" power of quantum cryptography, especially so that quantum attacks may be the next threat to cybersecurity (Denning, 2019).

Future Work

To ensure that Digital checking systems are customizable based on regulatory aspects, future work will have to consider modular capabilities which can be enabled or disabled based on the context of the application, including transferring e-checks, and such features as individual/corporate client preferences on transferability of the e-check. The online e-checking system should also consider bearers other than the designated payee in the case of transferred e-checks.

As earlier mentioned in the recommended enhancements, the future direction of research in online checking should focus on fortifying the vaunted "unbreakable" power of quantum cryptography, as Denning (2019) recommended. Quantum cryptography is an ace for

cybersecurity, and research to explore any possible weaknesses in the current approaches should be reinforced through supplementary safeguards to maintain the integrity of any financial technology developments anchored on it. Among the promising scientific approaches to research include a combination of data mining techniques and application of artificial intelligence to bolster the yet untapped strengths of quantum technology.

An important step in harnessing the advantages of the proposed process flow in the conclusion is to propose it to a financial technology innovation lab, preferably with The Ministry of Finance (MOF). The enhancements recommended in this capstone project is, admittedly, financially draining for an individual researcher. However, if the proposed system is approved for inclusion in the MOF's Innovation Lab, integrated support from financial institutions and the financial technology sector can serve as an incubator for a more secure online checking system. The benefits of a collaborative ecosystem fostered through financial technology innovation research can help catalyze a stronger barrier against fraud and cybersecurity breaches in the banking system.

References

1. Anderson, H., & Yull, S. (2012). *BTEC nationals - IT practitioners*. Routledge.
2. BBVA Innovation Center. (2012). *Innovation edge: Mobile banking*. Author.
3. Bu, C. (2018). Network security based on K-means clustering algorithm in data mining research. Proceedings of the 8th International Conference on Social Network, Communication and Education (SNCE 2018), 642-645. https://doi.org/10.2991/snce-18.2018.130
4. Carrera, A. (2020). *A macroeconomic analysis of profit*. Routledge.
5. Challenger, M., Tezel, B. T., Amarald, V., Goulão, M., & Kardas, G. (2021). Agent-based cyber-physical system development with SEA_ML++. In B. Tekinerdogan, D. Blouin, H. Vangheluwe, M. Goulão, P. Carreira, & V. Amaral (Eds.), *Multi-paradigm modelling approaches for cyber-physical systems* (pp. 195–219). Academic Press.
6. Chang, C. C., Chang, S. C., & Lee, J. S. (2009). An online electronic check system with mutual authentication. *Computers & Electrical Engineering*, *35*(5), 757–763. https://doi.org/10.1016/j.compeleceng.2009.02.007
7. Chaum, D., Fiat, A., & Naor, M. (1990a). Untraceable electronic cash (Extended abstract). In S. Goldwasser (Ed.), *Advances in cryptology - CRYPTO '88: Proceedings* (pp. 319-327). Springer.
8. Chaum, D., den Boer, B., van Heyst, E., Mjjolsnes, S., & Steenbeek, A. (1990b). Efficient offline electronic checks (Extended abstract). *Advances in Cryptology - Proceedings*, *434*, 294–301.
9. Chen, W. K. (2005). Efficient on-line electronic checks. *Applied Mathematics and Computation*, *162*(3), 1259–1263. https://doi.org/10.1016/j.amc.2004.03.006

10. Crepeau, C. (2019). Cut-and-choice protocol. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of cryptography and security* (2nd ed., p. 290). Springer.
11. Dlabay, L., Burrow, J. L., & Kleindl, B. (2018). *Principles of business updated* (9th precision exams ed.). Cengage Learning.
12. Doshi, H. (2020). *CISA–certified information systems auditor study guide*. Packt Publishing.
13. Ferguson, N. (1994). Single term off-line coins. *Advances in Cryptology: EUROCRYPT '93, 765*, 318–328.
14. Humphrey, D. V., & Hunt, R. (2012, May). *Getting rid of paper: Savings from Check 21* (No. 12–12). Federal Reserve Bank of Philadelphia. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.956.8711&rep=rep1&type=pdf
15. Jacob, K., Lunn, A., Porter, R. D., Rousse, W., Summers, B., & Walker, D. (2009). *Digital checks as electronic payment orders* (PDP 2009-5). Federal Reserve Bank of Chicago. https://www.chicagofed.org/-/media/publications/policy-discussion-papers/2009/pdp2009-5-pdf.pdf
16. Javid, T. (2018). Secure access to biomedical images. In C. Pradhan, H. Das, B. Naik, & N. Dey (Eds.), *Handbook of research on information security in biomedical signal processing* (pp. 38–53). Information Science Reference-IGI Global.
17. Kim, H. (2015). *Wireless communications systems design*. Wiley.
18. Kumar, V., Kumar, R., & Pandey, S. K. (2017, October). An enhanced and secured RSA public key cryptosystem algorithm using Chinese remainder theorem. In P. Bhattacharyya, H. G. Sastry, V. Marriboyina, & R. Sharma (Eds.), *Smart and innovative*

trends in next generation computing technologies (Revised Selected Papers, Part II) (pp. 543–554). Springer.

19. Lakshmi, M. A., Daniel, G. V., & Prasad, S. K. (2019). Initial centroids for K-means using nearest neighbors and feature means. In J. Wang, M. R. G. Reddy, K. V. Prasad, & S. V. Reddy (Eds.), *Soft computing and signal processing: Proceedings of ICSCSP 2018, Volume 1 (Advances in Intelligent Systems and Computing, 900)* (pp. 27–34). Springer.
20. Lee, J. K., & Yoon, H. S. (2000). An intelligent agents–based virtually defaultless check system: The SafeCheck system. *International Journal of Electronic Commerce*, *4*(3), 87–106. https://doi.org/10.1080/10864415.2000.11518373
21. Li, S. P. (2015). Hong Kong's experience in strengthening the security measures of retail payment services. In R. G. Smith, R. Cheung, & L. Y. Lau (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 165-181). Springer.
22. Linoff, G. S., & Berry, M. J. A. (2011). *Data mining techniques: For marketing, sales, and customer relationship management* (3rd ed.). Wiley.
23. Liu, J. K., Wong, S. H., & Wong, D. S. (2004, January). *A new e-check system*. Pennsylvania State University. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.543.9340
24. Lui, J. K., Wong, S. H., & Wong, D. S. (2005, June). Transferable e-cash revisit (A retitle of A new e-check system). In R. Sasaki, S. Qing, E. Okamoto, & H. Yoshiura (Eds.), *IFIP TC11 20th International Information Security Conference*. Springer.
25. McGlinn, A. (2005). Check Clearing for the 21st Century Act: The impact on consumers. *North Carolina Banking Institute*, *179*(1), 179–200. http://scholarship.law.unc.edu/ncbi/vol9/iss1/9

26. Paul, M. B., & Sharna, U. (2021). Security in cloud computing for sensitive data: Challenges & propositions. In D. Gupta, A. D. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, & A. Jaiswal (Eds.), *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 1 (Advances in Intelligent Systems and Computing, 1387)* (pp. 905–918). Springer.
27. Quinn, S., & Roberds, W. (2008). The evolution of the check as a means of payment: A historical survey. *Ferderal Reserve Bank of Atlanta: Economic Review, 93*(4), 1-28. https://www.econstor.eu/handle/10419/57670
28. Reingold, O., Trevisan, L., & Vadhan, S. (2004). Notions of reducibility between cryptographic primitives. In M. Naor (Ed.), Theory of cryptography: First theory of cryptography conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, proceedings (pp. 1-20). Springer Science & Business Media.
29. Rui, X. (2010). Secure e-check payment model based on ECC. *Proceedings of the 2010 WASE International Conference on Information Engineering*, *2010*(2), 109–112. https://doi.org/10.1109/ICIE.2010.121
30. Schmidt, J. W., & Brodie, M. L. (2011). *Relational database systems: Analysis and comparison*. Springer.
31. Seito, T., Aikawa, T., Shikata, J., & Matsumoto, T. (2010). Information-theoretically secure key-insulated multireceiver authentication codes. In D. J. Bernstein & T. Lange (Eds.), *Progress in Cryptology - AFRICACRYPT 2010: Third International Conference on Cryptology in Africa (Proceedings)* (pp. 148–165). Springer-Verlag.

32. Sertkaya, I., & Kalkar, O. (2021). A privacy enhanced transferable electronic checkbook scheme. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-09268-4

33. Shaheen, B., & Siddiqui, F. (2020). Comparison between RSA algorithm and modified RSA algortihm used in cloud computing. In S. Smys, R. Bestak, & Á. Rocha (Eds.), *Inventive computation technologies* (pp. 218–224). Springer Nature.

34. Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization. In A. E. Hassanien & M. Elhoseny (Eds.), Cybersecurity and secure information systems: Challenges and solutions in smart environments (pp. 31-42). Springer.

35. Sharma, N., Shamkuwar, M., Kumaresh, S., Singh, I., & Goje, A. (2021). Introduction to blockchain and distributed systems—fundamental theories and concepts. In S. Krishnan, V. E. Balas, J. Golden, H. Y. Robinson, & R. K. Mishra (Eds.), *Blockchain for smart cities* (pp. 183–210). Elsevier.

36. Sravanthi, D. V., & Rao, A. N. (2014). Application of data mining techniques for information security in a cloud. *International Journal of Engineering Research & Technology*, *2*(15), 218–224. https://www.ijert.org/application-of-data-mining-techniques-for-information-security-in-a-cloud

37. Starczewski, A., & Cader, A. (2020). Grid-based approach to determining parameters of the DBSCAN algorithm. In L. Rutkowski, R. Scherer, M. Korytkowski, W. Pedrycz, R. Tadeusiewicz, & J. M. Zurada (Eds.), *Artificial intelligence and soft computing: 19th International Conference, ICAISC 2020, Zakopane, Poland, October 12–14, 2020,*

Proceedings, Part II (Lecture Notes in Computer Science) (1st ed. 2020 ed., pp. 555–565). Springer.

38. Terrell, R. (2018). *Concurrency in .NET: Modern patterns of concurrent and parallel programming*. Manning.
39. Thorsteinson, P., & Ganesh, A. G. G. (2004). Digital signatures. In *.NET security and cryptography* (pp. 127–152). Pearson Hall Professional Technical Reference.
40. United States House of Representatives: Committee on Financial Services. (2006). *Implementation of the Check Clearing for the 21st Century*. US Government Printing Office.
41. Vadoodparast, M., Hamdam, A. R., & Sarim, H. M. (2015). Fraudulent electronic transaction detection using dynamic KDA model. *International Journal of Computer Science and Information Security*, *13*(3), 90–99.
42. Yoon, E.-J., & Yoo, K.-Y. (2005, December). Secure fingerprint-based remote user authentication scheme using smartcards. In X. Deng & Y. Ye (Eds.), *First International Workshop, WINE 2005 Proceedings* (pp. 405–413). Springer Verlag.
43. Zhang, P., He, Y., & Chow, K. P. (2018). Fraud track on secure electronic check system. *International Journal of Digital Crime and Forensics*, *10*(2), 137–144. https://doi.org/10.4018/ijdcf.2018040108
44. Toronto, C. E. (2020). Overview of the integrative review. In C. E. Toronto & R. Remington (Eds.), *A step-by-step guide to conducting an integrative review* (pp. 1–10). Springer Nature.
45. Auer, R. A., Comeli, G., & Frost, J. (2020). *Rise of the central bank digital currencies: Drivers, approaches and technologies* (CESifo Working Paper, No.8655). Center for

Economic Studies - Ifo Institute for Economic Research. https://www.econstor.eu/bitstream/10419/229473/1/cesifo1_wp8655.pdf

46. Goode, A. (2018). Biometrics for banking: Best practices and barriers to adoption. *Biometric Technology Today*, *2018*(10), 5-7. https://doi.org/10.1016/s0969-4765(18)30156-5
47. Whiskerd, N., Dittmann, J., & Vielhauer, C. (2018). A requirement analysis for privacy preserving biometrics in view of universal human rights and data protection regulation. *26th European Signal Processing Conference (EUSIPCO)*, 548-552.https://doi.org/10.23919/eusipco.2018.8553045
48. Sharbaf, M. S. (2009). Quantum cryptography: A new generation of information technology security system. *2009 Sixth International Conference on Information Technology: New Generations*, 1644-1648. https://doi.org/10.1109/itng.2009.173
49. Denning, D. (2019). Is quantum computing a cybersecurity threat? American Scientist, 107(2), 83. https://doi.org/10.1511/2019.107.2.83
50. Weinfurter, H. (2014). Principles of quantum cryptography/quantum key distribution (QKD) using attenuated light pulses. In S. Prawer & I. Aharonovich (Eds.), *Quantum information processing with diamond: Principles and applications* (pp. 21-35). Elsevier.
51. He, Q., & He, H. (2020). A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining. *Sustainability*, *13*(1), 101. https://doi.org/10.3390/su13010101
52. Sarker, I. H., Kayes, A., S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(41). https://doi.org/10.20944/preprints202006.0139.v1

53. Dennett, D. C. (2014). *Darwin's dangerous idea: Evolution and the meanings of life*. Simon & Schuster.

54. Ghassemian, D. (2017, November 17). *What exactly are echecks? Electronic checks demystified*. Tipalti. https://tipalti.com/echecks-for-global-payments/

55. Bidgoli, H. (2020). *MIS: Management information systems* (9th ed.). Mindtap - Cengage.

56. Blaney, B. (2020). The costs of check vs ACH payments. *Tipalti*. https://tipalti.com/check-vs-ach-costs/

57. Carnell, R. S., Macey, J. R., Miller, G. P., & Conti-Brown, P. (2021). *The law of financial institutions* (7th ed.). Aspen.

58. Mills, K. G. (2019). *Fintech, small business & the American dream: How technology is transforming lending and shaping a new era of small business opportunity*. Palgrave Macmillan - Springer Nature.

59. Rampton, J. (2022, January 22). *eChecks and international customers*. https://due.com/blog/ echecks-and-international-customers/

60. Mondonedo, M. (2020). *ACH payment processing*. Global Payments Integrated. https://www.globalpaymentsintegrated.com/en-us/blog/2021/02/02/ach-payment-processing

61. Belew, S., & Elad, J. (2020). *Starting an online business all-in-one for dummies.* (5th ed.). John Wiley & Sons.

62. Blaney, B. (2020). The costs of check vs ACH payments. *Tipalti*. https://tipalti.com/check-vs-ach-costs/

63. Gerdes, G. R., & Walton, J. K. (2002). The use of checks and other noncash payment instruments in the United States. *Federal Reserve Bulletin*, *88*(8), 360–374.

https://doi.org/10.17016/bulletin.2002.88-8

64. Guo, C., Chang, C.-C., & Chang, S.-C. (2018). A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications. *International Journal of Network Security*, *20*(2), 323–331. https://doi.org/10.6633 /IJNS.201803.20(2).13

65. Chiou, S.-F. E., Pan, H.-T., Cahyadi, E. F., & Hwang, M.-S. (2019). Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications. *International Journal of Network Security*, *21*(1), 100–104. https://doi.org/10.6633/IJNS.201901 21(1).12

66. Oney, E., Oksuzoglu Guven, G., & Hussain Rizvi, W. (2017). The determinants of electronic payment systems usage from consumers' perspective. *Economic Research (Ekonomska Istraživanja)*, *30*(1), 394–415. https://doi.org/10.1080/1331677x.2017.1305791

Appendix 1. Desirability as a Payment Instrument Evaluation Scale

Attribute	**Extent of Integration of the Six Desirable Characteristics**		
	Indicators	**Extent**	**Applicability**
Certainty (Jacob et al., 2009; Mills, 2018)	• Ability of banks to process e-checks within a reasonable period (24-48 hours or less).	***Low***	A few selected banks with global presence; much to be desired about legal framework in most countries
		Medium	Selected banks in some high-income and open-trade countries; present but

	• Strong legal framework to ensure value exchange		inadequate legal framework in some countries
		High	All banks in high-income and open-trade countries, and in some other countries; strong legal framework on the mentioned countries
		Very High	All banks/countries globally; strong legal framework globally.
Convenience (Jacob et al., 2009; Bidgoli, 2020; Carnell et al., 2021)	• Non-arduous processing for initiation and receipt; • Dependable record creation and maintenance	***Low***	A few selected banks with global presence
		Medium	Selected banks in some high-income and open-trade countries
		High	All banks in high-income and open-trade countries, and in some other countries
		Very High	All banks/countries globally
Economy (Jacob et al., 2009; Belew & Elad, 2017; Blaney, 2020)	• Acceptable and reasonable transaction costs of maintenance and operation • $0.26-0.50 (e-check) vs. $1.50 median (debit & credit cards).	***Low***	A few banks with global presence but with higher transaction costs
		Medium	Selected banks in some high-income and open-trade countries
		High	Almost all banks globally
		Very High	All banks globally
Information (Jacob et al., 2009; Mondonedo, 2020)	• Specific user knowledge and familiarity in processing/recording transactions; • Easy recognition of payee identification • Infallibility of authentication • Availability of information sources	***Low***	Familiarity: few users; for banks: moderate reliability of identification & authentication; lack of information sources.
		Medium	Familiarity: some user-types; for banks: moderate reliability of identification & authentication; abundance of information sources.
		High	Familiarity: almost all user-types; for banks: reliable identification & authentication; abundance of information sources.
		Very High	Familiarity: all user types globally; for banks: fool-proof identification & authentication; abundance of information sources.
Security (Jacob et al., 2009; Chiou et al., 2019; Guo et al., 2018; Zhang et al., 2018)	• Protection afforded to the transfer of value • Protection afforded to the supporting identity of transaction participants from data breach and fraud	***Low***	Some present threats neutralized, but others remain unchecked plus newer threats are evolving fast.
		Medium	Present security threats neutralized, but newer threats are evolving fast.
		High	Some present and near future security threats neutralized
		Very High	All present and near future security threats neutralized

Universality (Jacob et al., 2009; Ghas-emian, 2017; Oney, 2017; Cenusa, 2020)	• Wide acceptance of e-checks as a payment instrument by banks and majority of payors and payees • Availability of reliable infrastructure	***Low***	Accepted in some countries by many payment institutions, payees, and payors; Reliable infrastructure
		Medium	Accepted in many countries by most payment institutions, payees, and payors; Reliable infrastructure
		High	Globally accepted by most payment institutions, payees, and payors; Strong and reliable infrastructure
		Very High	Globally accepted by all payment institutions, payees, and payors; Strong, reliable, and consistently developing infrastructure