International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I8P107

Volume 69 Issue 8, 26-34, August 2021
© 2021 Seventh Sense Research Group®

Review Article

A Survey on Digital Payments Security: Recent Trends and Future Opportunities

Neha Priya[1], Jawed Ahmed[2]

[1]*M.Tech.CSE with specialization in Cyber Forensics and Information Security*

[2]*Assistant Professor, Department of Computer Science & Engineering, SEST, Jamia Hamdard, New Delhi, India.*

Received Date: 15 July 2021
Revised Date: 17 August 2021
Accepted Date: 29 August 2021

Abstract - *Digital payment technologies are growing very fast in the sector of e-commerce and mobile banking. This phenomenon has brought vast population to the cyber space for online payments. However, the users are often not aware of security aspects of online transactions. The banking regulations mandate technology led security interventions by intermediaries to protect customers from cyber fraud in digital payments ecosystem. Our literature survey shows the research trend in digital payments security for the past one decade. We use a literature classification framework for systematic literature review on the theme of this work. IS security can impact digital payments across three sectors- its growth motivation, growth challenges and growth assurance respectively. We discuss the recent trends to highlight the research gaps and potential security application areas. We review the literature across several prominent IT techniques used for digital payments security and suggest future opportunities.*

Keywords - *Cyber fraud, Digital payment, IS security, Mobile banking, Online payment, Systematic literature review.*

I. INTRODUCTION

Digital technology gives fast and convenient lives, but it comes at a cost- the threat of digital crimes. Even though there is considerable awareness about digital crimes, they continue to happen [1]. Further, digital services utilize cyberspace to replace traditional methods of work and business. The cyberspace is vulnerable to the risk of cyber crimes infiltrating online economic and social activities [2]. Banking industry has largely leveraged digital technology to devise diversified financial products and services [3]. A recent example is digital payment services in money and banking, which has given ‘convenience' as the key benefit and ‘security' as the key cost [4].

The digital payments ecosystem is a prudent example of Information Technology (IT) adoption in the domain of Information Systems (IS). Recent research trend on IT adoption shows that mobile technology (which includes mobile payments), e-commerce and internet banking are among the top five IT adoption contexts in research and mostly follow the Technology Acceptance Model (TAM) [5]. The technology acceptance of digital payments is dependent on factors affecting user attitude, intention and behaviour [6]. Besides, ease of use and perceived usefulness, trust and perceived risk are considered to be prominent behavioural factors affecting digital payments use [7]. Cyber frauds are identified as one of the risks in digital payments technology adopted by banks [8]. The incidence of cyber crime in online banking transactions on smart phones, shows that there are mostly victims of bank frauds cases, other cases being phishing and injection of malware [9]. Bank fraud here refers to an unauthorized online payment transaction. It is not only a cyber crime, but also a financial crime [10]. Therefore, we would alternatively refer to ‘cyber fraud in the digital payments ecosystem' as ‘digital payment fraud'.

For securing digital payment services, we understand that IT adoption can bring forth three broad scopes in security research, namely secured operations, security analysis, and security controls which form the basis of our literature classification framework. The objective of our work is to highlight the recent research trends for securing the digital payments ecosystem and find research gaps to enable IT researchers to get future research directions.

In the rest of this article, follows section 2 with related work to explain motivation for this work. Section 3 presents our literature classification framework and section 4 describes the research methodology. In section 5 we discuss the results to highlight recent trends. Section 6 presents reviews of selected literature to find research gaps. We conclude in section 7 with potential research opportunities.

II. RELATED WORK

There exists several literature reviews which discuss about security in any one of the digital payments technology areas, such as, mobile payments [11, 9, 12, 13] or payment cards [14, 15, 16]. We hold this observation from the reviews published in two research databases, the Springer Link and ScienceDirect, where these articles mentioned associated keywords in their title or abstract. In [11], authors explore the state of mobile payment technology access for elderly with major concerns including security, trust and privacy. In [9], a review on the vulnerabilities in android mobile phones for banking transactions is presented based on the incidence of attacks. In [12], a review on region specific adoption of mobile payments showed that the focus and grey areas include security technology and implementation. Another review on mobile payments adoption highlights initial trust and perceived risk as one of the driving factors for user acceptance [13]. For payment card fraud detection, AI and machine learning (ML) methods which are effective for use by industry, are reviewed in [14]. In [15], the author has discussed the scope of data mining techniques in preventing frauds in online card payments. In [16], authors compare ML techniques for predicting credit card fraud and their performance metrics.

The status of digital payments sector, as a whole, has not been reviewed comprehensively in the past decade from the perspective of security research. This research addresses the need for reviewing the emerging research trend in IT for securing digital payments ecosystem. Security is identified as one of the independent variables in IT adoption [5]. A distribution of independent variables over research trend, shows that ‘security’ has comparatively less research contributions, while another independent variable ‘trust’ has the fourth most prominent position in research [5]. However, in the context of digital payments, security cannot be looked independently of trust as shown by [17]. Banks hold relation of trust with their customers for ensuring protection of customers’ money through security solutions [18]. Security builds trust of customers in online banking and trust leads to positive growth [5, 19]. Therefore, we focus on the recent trends in IS security research for digital payments growth.

III. LITERATURE CLASSIFICATION FRAMEWORK

In this section, we define a three factors based literature classification framework which assess the impact of IS security research on digital payments growth. For a systematic review of literature from the past decade, this framework comprises following growth factors:

A. Growth Motivation

In this category, we classify those literature whose focus is on adoption of IT techniques in new product designs or updates, in order to ensure deployment of secured products.

B. Growth Challenges

This category refers to the need of technology to discover vulnerabilities and other growth challenges. Literature which address these challenges using IT techniques in research, are classified here.

C. Growth Assurance

The research focus area of literature classified into this category, includes IT techniques adopted for deployment of security controls which assure trust led growth in digital payments ecosystem.

IV. METHODOLOGY

We perform a systematic review based on the guidelines for literature review methodologies discussed in [20]. Our research method comprises five steps as shown in Fig. 1. It is drawn from the approaches suggested by [11] and [21]. First, the scope of review is defined to enable convergence of search results. The next step is searching in the literature databases, with suitable search string containing keywords. This is followed by screening of preliminary search results to narrow down the content for review. After screening, the selected research articles are represented in the form of illustrations to answer the review questions. The results are analysed and discussed.

A. Defining Scope

The goal of this literature review is to discover the research contributions in IT which have the potential to improve security solutions for digital payments. We aim to search and analyse research articles published in the last ten years since 2010, which are in scope of our literature classification framework.

B. Searching

The search process can be divided into these tasks: defining sources, developing search string and implementing search. The associated search areas are digital payment systems, Information Technology and security applications. The well known academic database ScienceDirect is selected as the literature source, due to its extensive coverage of the topic and its content search feasibility. In our literature search, we have included only those research articles which are published in journals or in conference proceedings. Both full-text as well as preview-only articles are retained in search results. We limit the search results to the discipline of IS or Computer Science.

C. Screening

The screening step is a filtering stage. It includes both exclusion and inclusion criteria for reducing the number of studies in our review, as shown in Fig. 2. First, we go through the title and keywords of 441 articles obtained from the search procedure and apply the exclusion criteria to 121 articles which are unrelated to ‘digital payment OR security research'. For the remaining 320 articles, we read their abstract and apply another exclusion criteria of research based on empirical findings. We also exclude, from our review, articles related to ‘digital money or virtual currency’ and articles related to ‘offline e-cash or conditional e-payment'. At this stage, we apply the inclusion criteria of articles related to ‘digital payments AND security research’. Finally, we obtained 64 articles after screening and read these literature for further investigation.

We construct our search string from keywords, as suggested in [21]. For efficient search, one word as well as two words based keywords are used. Literature reviews, discussed in this research so far, do not give exhaustive list of keywords to address our scope of review. So, we selectively combine keywords from [11], [9] and [14]. The resultant search string is:

(Mobile banking OR m-banking OR mobile payment OR m-payment OR online banking OR internet banking OR online payment OR electronic payment OR digital

payment OR online transaction OR digital transaction OR payment card OR credit card)

AND

(Security OR security control OR security measure OR intelligence OR payment fraud OR information technology)

Our preliminary search results gave 858 research articles, where 186 articles were available as full-text. We have to manually exclude articles not related to IS or Computer Science discipline by going through the title of their journal or proceedings. Consequently, we got 441 articles for further screening.

D. Research Questions

To begin with the review of literatures, two research questions are proposed for literature analysis. Our aim is to find the yearly distribution of selected articles over the literature classification framework by answering the following research questions:

- Which Security application areas are in focus of research?
- Which IT techniques are emerging areas of security research?

E. Analysis of Results

The goal of literature analysis is to identify prominent research gaps and potential research contributions. We analyse the results containing literature distribution and obtain an integrated outlook to the situation of security research for digital payments growth.

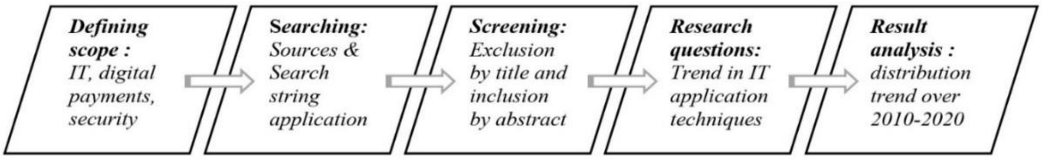
Defining scope :
IT, digital payments, security
Searching:
Sources & Search string application
Screening:
Exclusion by title and inclusion by abstract
Research questions:
Trend in IT application techniques
Result analysis :
distribution trend over 2010-2020

Fig. 1 Research methodology for systematic literature review

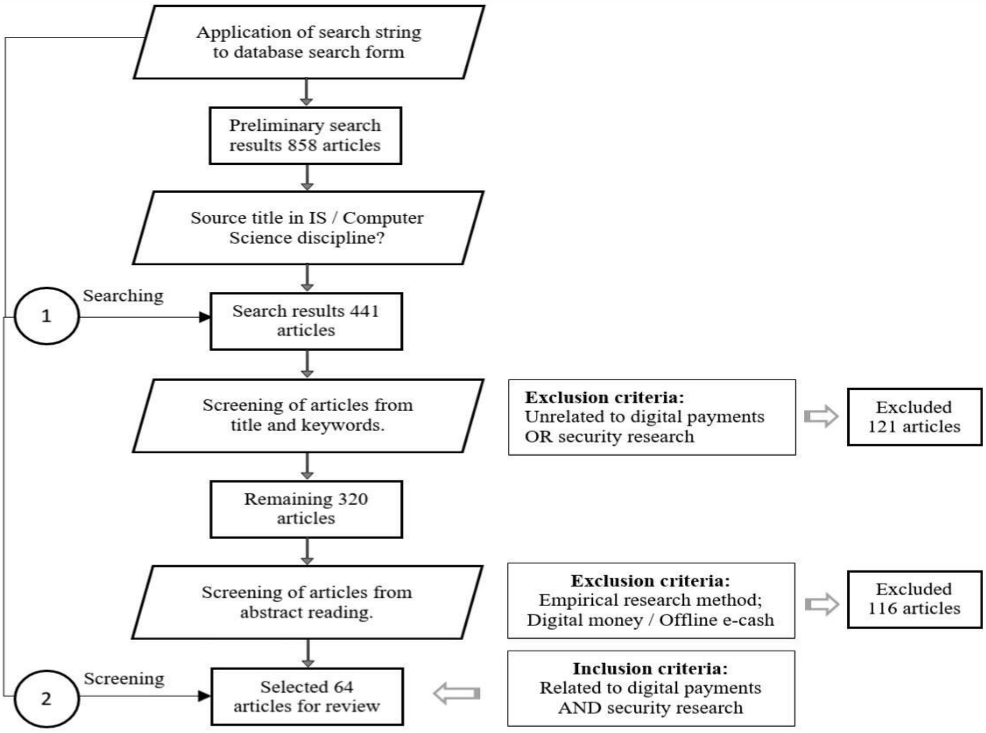
Application of search string to database search form
Preliminary search results 858 articles
Source title in IS / Computer Science discipline?
Searching
1
Search results 441 articles
Screening of articles from title and keywords.
Exclusion criteria:
Unrelated to digital payments OR security research
Excluded 121 articles
Remaining 320 articles
Screening of articles from abstract reading.
Exclusion criteria:
Empirical research method;
Digital money / Offline e-cash
Excluded 116 articles
Screening
2
Selected 64 articles for review
Inclusion criteria:
Related to digital payments AND security research

Fig. 2 Literature search and screening process chart

V. RESULTS AND DISCUSSION

Research articles are classified under three digital payment growth factors, namely growth motivation, growth challenges and growth assurance, according to our literature classification framework. For each growth factor, we further identify research contributions into various security application areas and corresponding IT techniques are also listed. Thus, we get the distribution of research articles to answer our research questions. Table 1 reveals that number of researches published is apparently high in five security application areas, in the order as Authentication mechanism; Fraud detection; Policy and law; Secure payment protocols; and Payment privacy.

We observe from Table 2 and Fig. 3 that over the closing decade (2010-2020), there is general expansion in use of IT techniques for securing digital payments ecosystem. It is notable that security led growth motivation is in rise over the second half of the decade. For addressing growth challenges, the research community appears to be making low but regular contribution over the decade. A more interesting observation has emerged from the third part of literature classification framework, the Growth assurance. Due to breakthrough IT techniques such as Machine learning and big data in the recent times, research work is concentrated in second half of this decade. Thus, the distribution of research articles highlight the trending security applications areas and their emerging IT techniques.

Table 1. Distribution of research articles as per literature classification framework

Framework	Security Application areas	IT Techniques	No. of articles

Growth Motivation
(32 articles)
	Authentication mechanism	Biometrics [23, 27, 40, 45, 68, 69];
		Elliptic curve cryptography (ECC) [30, 82];
		Key management [33, 64]; Graphical password[36];
		Cryptosystem [46, 47, 52, 62, 72]; Steganography [65];
		Signcryption [83]
			18

	Payment privacy	Digital Signature [24, 28, 77, 84];
		Secure Element (SE) in mobile device [81];
		2-paymrnt gateway based on cryptography [85];
			6

	Secure Payment Protocol	Encryption protocol [26, 51, 80]; Tokenset optimisation [32] Application layer message format [66]; ECC [67, 78]; Subliminal channels [76]	**8**
Growth Challenges (14 articles)	Cyber attack analysis	Digital forensics [25]; cryptanalysis [70]	2
	Skimming attack analysis	Computer forensics [44]	1
	Mobile app vulnerability	Mobile forensics [55]	1
	Phishing threat avoidance	Security awareness [43, 63]	2

	Policy and Law	Digital signature law [34];
		Payment Service Directives (PSD) [38, 49];
		Liability rules [48, 56]; Data protection [53];
		Service agreement [58]; Electronic evidence [60]
			8

Growth Assurance (18 articles)	Malware detection	Machine learning [22, 29, 74]	3
	Spoof attack detection	Biometric anti-spoofing [73]	1
	Detecting replicated 2-D codes	Watermark extraction [75]	1
	Phishing detection	Machine learning [35]; Genetic algorithm [61]; Fuzzy system [71]	3

	Fraud detection	Big data analytics [31, 59]; Wavelet transform [37];
		Data intelligence [39]; Machine learning [41, 50];
		Deep learning [42]; Sequence classification [54];
		Network analysis [57]; Semi-supervised clustering [79]
			10

Table 2. Distribution of research articles based on security application areas

	Growth Motivation				**Growth Challenges**						**Growth Assurance**					
Year of Publication	**No. of articles**	Authentication mechanism	Payment privacy	Secure payment Protocol	**No. of articles**	Cyber attack analysis	Skimming attack analysis	Mobile app vulnerability	Phishing threat	Policy and Law	**No. of articles**	Malware detection	Spoof attack detection	Detecting replicated 2-D	Phishing detection	Fraud detection
2010	**1**	27														
2011	**3**	82		66,76	**1**					34						
2012	**4**	52,83		26,80	**1**	70										
2013	**2**	36,72			**3**				63	48,6 0						
2014	**2**	33,65			**2**		44		43							
2015					**2**	25				58	**4**		73		71	57,

																79
2016	**8**	64,68	24,77, 81	51,32, 78	**2**					38,56	**2**			75	35	
2017	**4**	30,47	28,85		**1**			55								
2018	**3**	45,62	84		**1**					49	**5**	29				31, 59, 41, 54
2019	**3**	23,69		67							**6**	22, 74				37, 39, 50, 42
2020	**2**	40,46			**1**					53	**1**				61	
Total		**18**	**6**	**8**		2	1	1	2	**8**		3	1	1	3	**10**

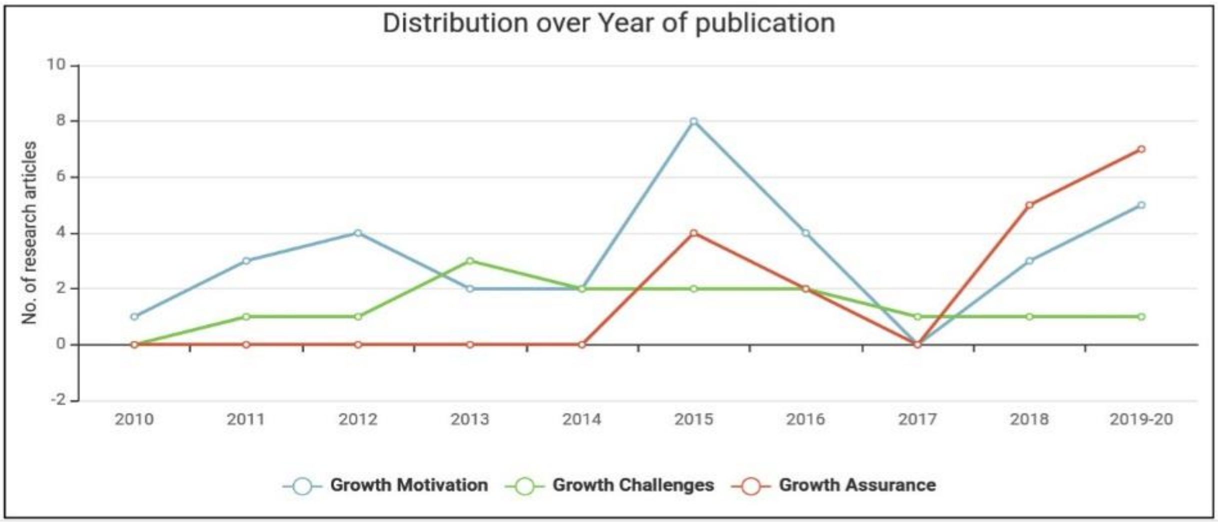

Fig. 3 Security research trend based on literature classification framework

VI. LITERATURE REVIEW

To find the research gaps, we have reviewed selected articles corresponding to each digital payment growth factor as defined in our literature classification framework. The emerging IT techniques for security research are emphasized for each contribution area.

A. Increasing Growth Motivation by security features

Security research on authentication, privacy and non-repudiation and payment protocols increase motivation for deployment of new products. Secured operation of digital payment transactions enable technology acceptance. Emerging research techniques in this area are:

a) Biometric Authentication

Biometric data such as fingerprints and face recognition are used for authentication of user accounts. It is more secure than traditional authentication mechanism based on alphanumeric passwords. However, biometric information need to be secured themselves. There is current research focus to improve reliability of biometric information used for authorizing online payments. In [68], (2016), authors propose finger, iris and palm print for physical biometrics and encrypt this data to prevent leak of sensitive data. In [40], (2020), authors emphasize on the future scope of voice or video selfie as biometrics, other than fingerprints, for authorization of online banking transactions. In a latest research topic on behavioural biometrics, keystroke dynamics is characterized and adjusted for aging effect to provide accuracy in authentication ([23], 2019). In [69], (2019), authors have proposed a continuous authentication mechanism which captures behavioural biometric data from sensors of android phones for in mobile banking application.

b) Cryptographic Security

Cryptography is commonly used in cryptosystems, key management tasks, encryption protocols and digital signatures. Cryptosystem provides security functions such as authentication, confidentiality and non-repudiation. When two different keys, the public and private key, are used in a cryptosystem, the technique is called asymmetric key cryptography. Security research trend shows that asymmetric key or public key algorithms have been a popular research area over the last decade. The use of elliptic curve cryptography is trending in security research for authentication of transactions and secured payment protocols [78, 30, 67]. Recent research topics based on the application of asymmetric key cryptography are: multi-layer encryption algorithms for improving security ([46], 2020); a certificate less encrypted signature for user authentication ([47], 2017); one-time username to replace predefined credentials for access control ([62], 2018); use of cryptography over 2 payment gateways for anonymity of mobile payments ([85], 2017). Key management is another important application area of public key cryptography. It depends on Public Key Infrastructure (PKI) for key generation and certification. The key research topics in the last decade were as: improving security of certificates distribution ([64], 2016); and use of partner key to eliminate the need for certificate validation ([33], 2014). Besides authentication, research for payment privacy and non-repudiation services are also in recent trend. Computational tasks, such as security verifications, are outsourced to a cloud server to save the limited resources of mobile devices. Since the outsourced cloud environment is unsecured, digital signature based payment protocols are one of the recent research topics, to improve anonymity and security of mobile wallet transactions [77, 28, 84].

B. Addressing Growth Challenges by Security Countermeasures

Growth challenges include vulnerabilities and threats in digital payments environment, past experiences of security attacks and existing security policy paralysis. Security analysis measures focus on identification of vulnerabilities, analysis of threats and attacks and review of critical policies or laws by security experts. Literature review results in Fig. 3 show consistent research efforts over the last decade to manage the growth challenges. However, the focus here is less than growth motivation or assurance contribution areas. Two emerging research techniques, namely digital forensics and security policy review are highlighted for future research directions.

a) Digital Forensics

Digital forensics research includes other sub-domains like computer forensics, mobile forensics and cyber forensics. With the growth of mobile payments, mobile apps are widely used. Mobile forensics research can enable analysis of any security attacks on the mobile devices. Digital forensic techniques may not only be used for post-incident analysis but also for validation of potential threats before an actual attack could take place [55].

b) Policy Evaluation

The area of security policy includes formulation and alteration of rules, regulations, guidelines, directives, laws issued by competent authorities with validity over a certain jurisdiction and timeframe. The policy research trend for digital payments domain relates to the current issues and concerns of the stakeholders, such as: liability ownership and the burden of proof [56], security authentication services [38], consumer protection through service agreement [58]. When the European Union mandated all banks to provide application programming interface or API so that third party payment system operators (PSO) could manage online payments by customers, this raised the issue of cybersecurity for customer's financial data [49]. A most recent policy research topic is evaluation of personal data protection regulations in digital payments ecosystem [53]. Existing policy and laws are growth challenges, given the evolving Financial technology (FinTech) sector. Future research directions include analysis of global and regional security conditions to suggest policy reforms.

C. Building Growth Assurance by Security Controls

The elements of growth assurance include additional security controls over normal operations of digital payment services. The primary goal of security applications is detection of cyberattacks on online payments, which are also financial crimes. Various classification algorithms are used in research for prediction of attacks and performance evaluation. Emerging IT techniques are machine learning, soft computing and big data analytics.

a) Machine Learning

Recent trend shows wide use of ML algorithms for detection of credit card frauds, phishing websites in internet banking and malwares in mobile applications. In [50], credit card frauds are detected in streaming transactions, by analysing each transaction and sending feedback for learning past transactional patterns. With the evolution of mobile payments technology, malware detection in android applications is a potential research area [22, 29, 74]. Research method for selection of a ML algorithm for the model, uses performance comparisons of different ML algorithms to determine the best model [22, 50].

b) Soft Computing

Even though, machine learning techniques are widely in binary classification problems, certain data limitations exist such as insufficient data and uncertainty. Soft computing techniques are utilized in ML problems with uncertainty and approximation of data. In [41], the fraud classifier is customized by a hyper-heuristic evolutionary algorithm which automatically selects components of the classifier model to suit the nature of input datasets. Another fraud classification problem is training data imbalance since the class of frauds is of much smaller size than the class of genuine transactions. In [42], authors have proposed a generative deep learning model to augment the data in fraud class for supervised machine learning. Soft computing techniques increase the effectiveness of fraud predictions. For detection of phishing attacks, features extraction and feature selection algorithms are important research areas in soft computing. In [71], phishing indicators are identified from Iranian e-banking websites and a fuzzy expert system is used for phishing detection. In [61] A genetic algorithm based feature selection method is proposed for classification of phishing websites.

c) Big Data Analytics

The volume of online payment transactions is increasingly large streaming data input for fraud prediction. Big data tools are integrated with machine learning algorithm, for scalability of fraud prediction models [59]. A big data interface, Hadoop, is used for storage and processing of the transactions data from the source to an analytical server, for prediction modelling. This approach increases the prediction performance of the ML algorithm used for classification [31]. To overcome data imbalance in big data problem, in [39] the authors have proposed a data intelligence based multiple consensus model, where probabilistic and majority voting of classification algorithms is combined for in large real dataset.

The digital payments' growth challenges continue to exist with the evolving information and communications technology (ICT). Hence, there remains the scope of persistent research directions arising from this sector. Financial and cyber crimes in digital payments, one of the growth challenges, are addressed by crime analysis, an important research topic in security. At this point, we make a note that security contributions, under Growth assurance, are making constant effort to detect and prevent crime events in real time. This lowers the incidence of crime and consequently, the activity burden of crime analysis is also reduced. Taking inspiration from this, we suggest a research direction where the crime analysis efforts can be further eased by using Growth assurance techniques such as data intelligence. Recent trend shows that data intelligence is an emerging but less researched technique for fraud detection. We suggest that, data intelligence can be utilized for fraud data analytics during investigation of crime cases. The volume of crime data is not big data. Therefore, crime data intelligence is a potential future research direction for disposal of crime cases in digital payments and also, in general cyber crimes, reported for investigation.

VII. CONCLUSION

The purpose of our literature review was to find security research trend over the past decade in the field of digital payments. The proposed systematic literature review methodology was used to define the research scope and important research questions. It provided an effective literature search and screening process. The literature classification framework represented research articles from different security perspectives. Our review results help us to discover past decadal research trend, current research gaps and future research directions. Since, research under Growth assurance has been at high rising trend recently, security applications under this head are promising research themes, especially fraud detection. The digital payments' growth challenges combined with growth assurance factors have scope of future IS security research. Areas where research contribution is low, such as cyber forensics and data intelligence, are potential research opportunities.

This work has used only selective databases and therefore, the trend outcome may be limited by the types of documents and databases used for literature survey. There is scope to combine the research trends with real life digital payments statistics, like volume of transactions or cyber fraud incidence, for better understanding of research problems.

ACKNOWLEDGMENT

We acknowledge the use of online databases at SpringerLink and ScienceDirect for browsing scientific documents. The line chart in this work was constructed using online drawing tool and workspace of Visual Paradigm Online.

REFERENCES

[1] A. Bancroft, Why Digital Crime Works, in The Darknet and Smarter Crime, Palgrave Studies in Cybercrime and Cybersecurity. (2020) 197–203. https://doi.org/10.1007/978-3-030-26512-0_11.

[2] A. Bancroft, Crime Is as Smart and as Dumb as the Internet, in: The Darknet and Smarter Crime, Palgrave Studies in Cybercrime and Cybersecurity. (2020) 197–203. https://doi.org/10.1007/978-3-030-26512-0_1.

[3] Jasmeet and A. Chandhok, Developments in Banking after Privatisation, Impact of Privatization on the Public Sector Banks, M.Phil (Management) thesis, Markandeshwar Institute of Management, Ambala, India, (2013). http://hdl.handle.net/10603/11205.

[4] Y. C. Shen, C. Y. Huang, C. H. Chu, and C. T. Hsu, A benefit cost perspective of the consumer adoption of the mobile banking system, Behaviour & Information Technology. 29 (5) (2010) 497–511. https://doi.org/10.1080/01449290903490658.

[5] M. Salahshour Rad, M. Nilashi, and H. Mohamed Dahlan, Information technology adoption: a review of the literature and classification, Universal Access in the Information Society. 17 (2018) 361–390. https://doi.org/10.1007/s10209-017-0534-z.

[6] J. C. Gu, S. C. Lee, and Y. H. Suh, Determinants of behavioral intention to mobile banking, Expert Systems with Applications. 36 (9) (2009) 11605–11616. https://doi.org/10.1016/j.eswa.2009.03.024.

[7] I. Bashir, and C. Madhavaiah, Consumer attitude and behavioural intention towards Internet banking adoption in India, Journal of Indian Business Research. 7 (1) (2015) 67–102. https://doi.org/10.1108/JIBR-02-2014-0013.

[8] G Gopalakrishna, G.Sivakumar, Patric Kishore, Akhilesh Tuteja, Kamlesh Bajaj, H.Krishnamurthy, Nandkumar Saravade, Abhay Gupte, B.Sambamurthy, Pavan Duggal, Sanjay Sharma, K.Ramakrishnan, and P.K.Panda Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Report and recommendations, Reserve Bank of India, Mumbai, (2011). https://rbidocs.rbi.org.in › PdfsPDF.

[9] P. F. Ordoñez-Ordoñez, D. D. Herrera-Loaiza, and R. Figueroa-Diaz, Vulnerabilities in Banking Transactions with Mobile Devices Android: A Systematic Literature Review, in: Botto-Tobar M., Pizarro G., Zúñiga-Prieto M., D'Armas M., Zúñiga Sánchez M. (eds) Technology Trends, CITT 2018, Communications in Computer and Information Science. 895 (2019) . https://doi.org/10.1007/978-3-030-05532-5_8.

[10] CDAC, Cyber Security Handbook for Digital Financial Transactions, in Information Security Education & Awareness, MeiTy. [Online]. Available: https://www.comprompt.co.in/financial-security/.

[11] N. T. Msweli, and T. Mawela, Enablers and Barriers for Mobile Commerce and Banking Services Among the Elderly in Developing Countries: A Systematic Review, in: Hattingh M., Matthee M., Smuts H., Pappas I., Dwivedi Y., Mäntymäki M. (eds) Responsible Design, Implementation and Use of Information and Communication Technology, I3E 2020, Lecture Notes in Computer Science. 12067 (2020). https://doi.org/10.1007/978-3-030-45002-1_27.

[12] R. Boateng, and M. Y. P. Sarpong, A Literature Review of Mobile Payments in Sub-Saharan Africa, in: Dwivedi Y., Ayaburi E., Boateng R., Effah J. (eds) ICT Unbounded, Social Impact of Bright ICT Adoption, TDIT 2019, IFIP Advances in Information and Communication Technology. 558 (2019). https://doi.org/10.1007/978-3-030-20671-0_9.

[13] Gonçalo Baptista, and Tiago Oliveira, A weight and a meta-analysis on mobile banking acceptance research, Computers in Human Behavior. 63 (2016) 480-489. https://doi.org/10.1016/j.chb.2016.05.074.

[14] Nick F. Ryman-Tubb, Paul Krause, and Wolfgang Garn, How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark, Engineering Applications of Artificial Intelligence. 76 (2018) 130-157. https://doi.org/10.1016/j.engappai.2018.07.008.

[15] D. Maheshwari, Payment Card Fraud Detection with Data Mining: A Review, in: Kumar A., Paprzycki M., Gunjan V. (eds) ICDSMLA 2019, Lecture Notes in Electrical Engineering. 601 (2020) . https://doi.org/10.1007/978-981-15-1420-3_164.

[16] C. V. Priscilla, and D. P. Prabha, Credit Card Fraud Detection: A Systematic Review, in: Jain L., Peng SL., Alhadidi B., Pal S. (eds) Intelligent Computing Paradigm and Cutting-edge Technologies, ICICCT 2019, Learning and Analytics in Intelligent Systems. 9 (2019). https://doi.org/10.1007/978-3-030-38501-9_29.

[17] B. Vatanasombut, M. Igbaria, A. C. Stylianou, and W. Rodgers, Information systems continuance intention of web-based applications customers: the case of online banking, Information & Management. 45 (2008) 419–428. https://doi.org/10.1016/j.im.2008.03.005.

[18] M. K. Jain, Consumer Protection in a digital Financial World – Initiatives and Beyond, in Annual Conference of Banking Ombudsman, 2019, RBI Bulletin August 2019.

[19] S. Goudarzi, W. H. Hassan, M. A. R. Baee, and S. Soleymani, The Model of Customer Trust for Internet Banking Adoption, in: Borowik G., Chaczko Z., Jacak W., Łuba T. (eds) Computational Intelligence and Efficiency in Engineering Systems, Studies in Computational Intelligence. 595 (2015). https://doi.org/10.1007/978-3-030-45002-1_27.

[20] Hannah Snyder, Literature review as a research methodology: An overview and guidelines, Journal of Business Research. 104 (2019) 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

[21] M. Eggert, and J. Alberts, Frontiers of business intelligence and analytics 3.0: a taxonomy-based literature review and research agenda, Business Research. (2020). https://doi.org/10.1007/s40685-020-00108-y.

[22] Ali Gezer, Gary Warner, Clifford Wilson, and Prakash Shrestha, A flow-based approach for Trickbot banking trojan detection, Computers & Security. 84 (2019) 179-192. https://doi.org/10.1016/j.cose.2019.03.013.

[23] Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara, Double serial adaptation mechanism for keystroke dynamics authentication based on a single password, Computers & Security. 83 (2019) 151-166. https://doi.org/10.1016/j.cose.2019.02.002.

[24] Jieling Wu, Chenglian Liu, and Donald Gardner, A Study of Anonymous Purchasing Based on Mobile Payment System, Procedia Computer Science. 83 (2016) 685-689. https://doi.org/10.1016/j.procs.2016.04.152.

[25] Muhammad Shamraiz Bashir, and Muhammad Naeem Ahmed Khan, A triage framework for digital forensics, Computer Fraud & Security. 2015(3)(2015)8-18. https://doi.org/10.1016/S1361-3723(15)30018-X.

[26] Wenmin Li, Qiaoyan Wen, Qi Su, and Zhengping Jin, An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network, Computer Communications. 35 (2)(2012) 188-195. https://doi.org/10.1016/j.comcom.2011.09.003.

[27] Anthony J. Palmer, Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA), Computers & Security. 29 (7) (2010) 785-806. https://doi.org/10.1016/j.cose.2010.03.002.

[28] Zhen Qin, Jianfei Sun, Abubaker Wahaballa, Wentao Zheng, Hu Xiong, and Zhiguang Qin, A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing, Computer Standards & Interfaces. 54 (1) (2017) 55-60. https://doi.org/10.1016/j.csi.2016.11.012.

[29] Harris Papadopoulos, Nestoras Georgiou, Charalambos Eliades, and Andreas Konstantinidis, Android malware detection with unbiased confidence guarantees, Neurocomputing. 280 (2018) 3-12. https://doi.org/10.1016/j.neucom.2017.08.072.

[30] Preeti Chandrakar, and Hari Om, A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC, Computer Communications. 110 (2017) 26-34. https://doi.org/10.1016/j.comcom.2017.05.009.

[31] Suraj Patil, Varsha Nemade, and Piyush Kumar Soni, Predictive Modelling For Credit Card Fraud Detection Using Data Analytics, Procedia Computer Science. 132 (2018) 385-395. https://doi.org/10.1016/j.procs.2018.05.199.

[32] Barbara Carminati, Elena Ferrari, and Ngoc Hong Tran, Trustworthy and effective person-to-person payments over multi-hop MANETs, Journal of Network and Computer Applications. 60 (2016) 1-18. https://doi.org/10.1016/j.jnca.2015.11.011.

[33] Glenn Benson, Shiu-Kai Chin, Sean Croston, Karthick Jayaraman, and Susan Older, Banking on interoperability: Secure, interoperable credential management, Computer Networks. 67 (2014) 235-251. https://doi.org/10.1016/j.comnet.2014.03.024.

[34] Hartini Saripan, and Zaiton Hamin, The application of the digital signature law in securing internet banking: Some preliminary evidence from Malaysia, Procedia Computer Science. 3 (2011) 248-253. https://doi.org/10.1016/j.procs.2010.12.042.

[35] Mahmood Moghimi, and Ali Yazdian Varjani, New rule-based phishing detection method, Expert Systems with Applications. 53 (2016) 231-242. https://doi.org/10.1016/j.eswa.2016.01.028.

[36] Sadiq Almuairfi, Prakash Veeraraghavan, and Naveen Chilamkurti, A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices, Mathematical and Computer Modelling. 58 (1–2) (2013) 108-116. https://doi.org/10.1016/j.mcm.2012.07.005.

[37] Roberto Saia, and Salvatore Carta, Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks, Future Generation Computer Systems. 93 (2019) 18-32. https://doi.org/10.1016/j.future.2018.10.016.

[38] Mary Donnelly, Payments in the digital market: Evaluating the contribution of Payment Services Directive II, Computer Law & Security Review. 32 (6) (2016) 827-839. https://doi.org/10.1016/j.clsr.2016.07.003.

[39] Salvatore Carta, Gianni Fenu, Diego Reforgiato Recupero, and Roberto Saia, Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model, Journal of Information Security and Applications. 46 (2019) 13-22. https://doi.org/10.1016/j.jisa.2019.02.007.

[40] Stuart Dobbie, Challenge of biometric security for banks, Biometric Technology Today. 2020 (3) (2020) 5-7. https://doi.org/10.1016/S0969-4765(20)30037-0.

[41] Alex G. C. de Sá, Adriano C.M. Pereira, and Gisele L. Pappa, A customized classification algorithm for credit card fraud detection, Engineering Applications of Artificial Intelligence. 72 (2018) 21-29. https://doi.org/10.1016/j.engappai.2018.03.011.

[42] Ugo Fiore, Alfredo De Santis, Francesca Perla, Paolo Zanetti, and Francesco Palmieri, Using generative adversarial networks for improving classification effectiveness in credit card fraud detection, Information Sciences. 479 (2019) 448-455. https://doi.org/10.1016/j.ins.2017.12.030.

[43] Nalin Asanka, Gamagedara Arachchilage, and Steve Love, Security awareness of computer users: A phishing threat avoidance perspective, Computers in Human Behavior. 38 (2014) 304-312. https://doi.org/10.1016/j.chb.2014.05.046.

[44] T. Souvignet, J. Hatin, F. Maqua, D. Tesniere, P. L. Ãger, and R. Hormi Ãre, Payment card forensic analysis: From concepts to desktop and mobile analysis tools, Digital Investigation. 11 (3) (2014) 143-153. https://doi.org/10.1016/j.diin.2014.06.006.

[45] Obi Ogbanufe, and Dan J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems. 106 (2018) 1-14. https://doi.org/10.1016/j.dss.2017.11.003.

[46] P. Dijesh, Suvanam Sasidhar Babu, and Yellepeddi Vijayalakshmi, Enhancement of e-commerce security through asymmetric key algorithm, Computer Communications. 153 (2020) 125-134. https://doi.org/10.1016/j.comcom.2020.01.033

[47] Jun Song, Fan Yang, and Lizhe Wang, Secure authentication in motion: A novel online payment framework for drive-thru Internet, Future Generation Computer Systems. 76 (2017) 146-158. https://doi.org/10.1016/j.future.2016.06.011.

[48] Nicole S. van der Meulen, You've been warned: Consumer liability in Internet banking fraud, Computer Law & Security Review. 29 (6) (2013) 713-718. https://doi.org/10.1016/j.clsr.2013.09.007.

[49] Mark Noctor, PSD2: Is the banking industry prepared?, Computer Fraud & Security. 2018 (6) (2018) 9-11. https://doi.org/10.1016/S1361-3723(18)30053-8.

[50] Vaishnavi Nath Dornadula, and S Geetha, Credit Card Fraud Detection using Machine Learning Algorithms, Procedia Computer Science. 165 (2019) 631-641. https://doi.org/10.1016/j.procs.2020.01.057.

[51] Mohamad Badra, and Rouba Borghol Badra, A Lightweight Security Protocol for NFC-based Mobile Payments, Procedia Computer Science. 83 (2016) 705-711. https://doi.org/10.1016/j.procs.2016.04.156.

[52] Saad M. Darwish, and Ahmed M. Hassan, A model to authenticate requests for online banking transactions, Alexandria Engineering Journal. 51 (3) (2012) 185-191. https://doi.org/10.1016/j.aej.2012.02.005.

[53] Yuanxin Li, and Darina Saxunov, A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations, Procedia Computer Science. 170 (2020) 1110-1115. https://doi.org/10.1016/j.procs.2020.03.060.

[54] Johannes Jurgovsky, Michael Granitzer, Konstantin Ziegler, Sylvie Calabretto, Pierre-Edouard Portier, Liyun He-Guelton, and Olivier Caelen, Sequence classification for credit-card fraud detection, Expert Systems with Applications. 100 (2018) 234-245. https://doi.org/10.1016/j.eswa.2018.01.037.

[55] Christian J. DâOrazio, and Kim-Kwang Raymond Choo, A technique to circumvent SSL/TLS validations on iOS devices, Future Generation Computer Systems. 74 (2017) 366-374. https://doi.org/10.1016/j.future.2016.08.019.

[56] Se-Hak Chun, Wooje Cho, and Ramanath Subramanyam, Transaction security investments in online marketplaces: An analytical examination of financial liabilities, Decision Support Systems. 92 (2016) 91-102. https://doi.org/10.1016/j.dss.2016.09.015.

[57] Véronique Van Vlasselaer, Cristián Bravo, Olivier Caelen, Tina Eliassi-Rad, Leman Akoglu, Monique Snoeck, and Bart Baesens, APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions, Decision Support Systems. 75 (2015) 38-48. https://doi.org/10.1016/j.dss.2015.04.013.

[58] Yue Liu, Consumer protection in mobile payments in China: A critical analysis of Alipay's service agreement, Computer Law & Security Review. 31 (5) (2015) 679-688. https://doi.org/10.1016/j.clsr.2015.05.009.

[59] Fabrizio Carcillo, Andrea Dal Pozzolo, Yann-AÃ Le Borgne, Olivier Caelen, Yannis Mazzer, and Gianluca Bontempi, SCARFF: A scalable framework for streaming credit card fraud detection with spark, Information Fusion. 41 (2018) 182-194. https://doi.org/10.1016/j.inffus.2017.09.005.

[60] Stephen Mason, Electronic banking and how courts approach the evidence, Computer Law & Security Review. 29 (2) (2013) 144-151. https://doi.org/10.1016/j.clsr.2013.01.003.

[61] Priya Saravanan, and Selvakumar Subramanian, A Framework for Detecting Phishing Websites using GA based Feature Selection and ARTMAP based Website Classification, Procedia Computer Science. 171 (2020) 1083-1092. https://doi.org/10.1016/j.procs.2020.04.116.

[62] Abdulrahman Alhothaily, Arwa Alrawais, Chunqiang Hu, and Wei Li, One-Time-Username: A Threshold-based Authentication System, Procedia Computer Science. 129 (2018) 426-432. https://doi.org/10.1016/j.procs.2018.03.019.

[63] Nalin Asanka, Gamagedara Arachchilage, and Steve Love, A game design framework for avoiding phishing attacks, Computers in Human Behavior. 29 (3) (2013) 706-714. https://doi.org/10.1016/j.chb.2012.12.018.

[64] Sundeuk Kim, Hyun-Taek Oh, and Young-Gab Kim, Certificate sharing system for secure certificate distribution in mobile environment, Expert Systems with Applications. 44 (2016) 67-77. https://doi.org/10.1016/j.eswa.2015.09.003.

[65] Soon-Nyean Cheong, Huo-Chong Ling, and Pei-Lee Teh, Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system, Expert Systems with Applications. 41 (7) (2014) 3561-3568. https://doi.org/10.1016/j.eswa.2013.10.060.

[66] Maria-Dolores Cano, and Gines Domenech-Asensi, A secure energy-efficient m-banking application for mobile devices, Journal of Systems and Software. 84 (11) (2011) 1899-1909. https://doi.org/10.1016/j.jss.2011.06.024.

[67] Sriramulu Bojjagani, and V.N. Sastry, A secure end-to-end proximity NFC-based mobile payment protocol, Computer Standards & Interfaces. 66 (2019) 103348. https://doi.org/10.1016/j.csi.2019.04.007.

[68] R. Malathi, and R. Jeberson Retna Raj, An Integrated Approach of Physical Biometric Authentication System, Procedia Computer Science. 85 (2016) 820-826. https://doi.org/10.1016/j.procs.2016.05.271.

[69] Okan Engin Basar, Gulfem Alptekin, Hasan Can Volaka, Mustafa Isbilen, and Ozlem Durmaz Incel, Resource Usage Analysis of a Mobile Banking Application using Sensor-and-Touchscreen-Based Continuous Authentication, Procedia Computer Science. 155 (2019) 185-192. https://doi.org/10.1016/j.procs.2019.08.028.

[70] Tae Hyun Kim, ChangKyun Kim, and IlHwan Park, Side channel analysis attacks using AM demodulation on commercial smart cards with SEED, Journal of Systems and Software. 85 (12) (2012) 2899-2908. https://doi.org/10.1016/j.jss.2012.06.063.

[71] Gholam Ali Montazer, and Sara Arab Yarmohammadi, Detection of phishing attacks in Iranian e-banking using a fuzzy–rough hybrid system, Applied Soft Computing. 35 (2015) 482-492. https://doi.org/10.1016/j.asoc.2015.05.059.

[72] Haowei Su, Xiaoli Wen, and Dabi Zou, A Secure Credit Recharge Scheme for Mobile Payment System in Public Transport, IERI Procedia. 4 (2013) 303-308. https://doi.org/10.1016/j.ieri.2013.11.043

[73] Mark Cornett, Can liveness detection defeat the m-commerce hackers?, Biometric Technology Today. 2015 (10) (2015) 9-11. https://doi.org/10.1016/S0969-4765(15)30157-0.

[74] Shikha Badhani, and Sunil K. Muttoo, CENDroid—A cluster-ensemble classifier for detecting malicious Android applications, Computers & Security. 85 (2019) 25-40. https://doi.org/10.1016/j.cose.2019.04.004.

[75] Satoshi Ono, Takeru Maehara, and Kazunari Minami, Coevolutionary design of a watermark embedding scheme and an extraction algorithm for detecting replicated two-dimensional barcodes, Applied Soft Computing. 46 (2016) 991-1007. https://doi.org/10.1016/j.asoc.2015.11.001.

[76] Chin-Ling Chen, and Jyun-Jie Liao, A fair online payment system for digital content via subliminal channel, Electronic Commerce Research and Applications. 10 (3) (2011) 279-287. https://doi.org/10.1016/j.elerap.2010.09.001.

[77] Jen-Ho Yang, and Pei-Yu Lin, A mobile payment mechanism with anonymity for cloud computing, Journal of Systems and Software. 116 (2016) 69-74. https://doi.org/10.1016/j.jss.2015.07.023.

[78] Khaleel Ahmad, and Md Shoaib Alam, E-commerce Security through Elliptic Curve Cryptography, Procedia Computer Science. 78 (2016) 867-873. https://doi.org/10.1016/j.procs.2016.05.549.

[79] Michele Carminati, Roberto Caron, Federico Maggi, Ilenia Epifani, and Stefano Zanero, BankSealer: A decision support system for online banking fraud analysis and investigation, Computers & Security. 53 (2015) 175-186. https://doi.org/10.1016/j.cose.2015.04.002.

[80] Jesús Téllez Isaac, and Sherali Zeadally, An Anonymous Secure Payment Protocol in a Payment Gateway Centric Model, Procedia Computer Science. 10 (2012) 758-765. https://doi.org/10.1016/j.procs.2012.06.097.

[81] Jia Ning Luo, Ming Hour Yang, and Szu-Yin Huang, An Unlinkable Anonymous Payment Scheme based on near field communication, Computers & Electrical Engineering. 49 (2016) 198-206. https://doi.org/10.1016/j.compeleceng.2015.08.007.

[82] SK Hafizul Islam, and G.P. Biswas, A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Journal of Systems and Software. 84 (11) (2011) 1892-1898. https://doi.org/10.1016/j.jss.2011.06.061.

[83] Arpita Mazumdar, and Debasis Giri, On-line Electronic Payment System using signcryption, Procedia Technology. 6 (2012) 930-938. https://doi.org/10.1016/j.protcy.2012.10.113.

[84] Yongjian Liao, Yichuan He, Fagen Li, and Shijie Zhou, Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement, Computer Standards & Interfaces. 56 (2018) 101-106. https://doi.org/10.1016/j.csi.2017.09.008.

[85] Venkatasamy Sureshkumar, R. Anitha, N. Rajamanickam, and Ruhul Amin, A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity, Computers & Electrical Engineering. 57 (2017) 223-240. https://doi.org/10.1016/j.compeleceng.2016.07.014.