AFRICA DEVELOPMENT AND RESOURCES RESEARCH INSTITUTE (ADRRI) JOURNAL

*ADRRI JOURNAL (***www.adrri.org***)*

pISSN: 2343-6662 ***ISSN-L***: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

Identity Fraud: A Literature Review and Future Research Directions

Joel Cherus[1*], Jason Githeko[2], Joseph Siror[2], Kageni Njagi[1]

[1]School of Science, Engineering & Technology, Kabarak University, Private Bag - 20157 Kabarak, Kenya

[2]Department of Computer Science, Egerton University, P.O. Box 536 Egerton 20115, Kenya.

Correspondence: cheruskimeli@googlemail.com

Received: 10th January, 2014 **Accepted**: 16th February, 2014 **Published Online:** 28th February, 2014

URL: http://www.adrri.org/journal

[**Cite as**: Joel, C., Jason, G., Joseph, S., and Kageni, N. (2014). Identity Fraud: A Literature Review and Future Research Directions. Africa Development and Resources Research Institute Journal, Vol. 5, No. 5(2), Pp. 36-53.]

Abstract

Identity fraud has been reported as one of the fastest growing crimes in the world today, and a key facilitator of terrorism, money laundering and trafficking (of people, drugs, weapons and illicit material). In the last few years, there has been a significant increase of academic research on the subject. It is important to establish the adequacy of exiting literature. This academic literature targets to explain the trends and methods as well as future risks and implications related to identity fraud. The aim of the review is to survey the literature and identify gaps in coverage and methodology and thus areas requiring future research. A standard systematic literature review method that involved a search of academic articles from digital libraries was used. A total of 120 articles were selected and a content analysis was performed on the identity fraud phenomenon which led to the identification of thematic areas. These thematic areas are (i) technical issues, (ii) policy and legal issues, (iii) trends, (iv) target sectors and (v) type of research. The analysis of these papers provides useful

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

insights into the anatomy of identity fraud. It is hoped that this review will be a good resource for anyone who is interested in undertaking identity fraud research.

Keywords: identity fraud, literature review, future research directions

INTRODUCTION

Contemporary forms of crimes are becoming increasingly sophisticated. Some of these crimes have become facilitators of other crimes. Identity fraud is one such crime that facilitates terrorism, money laundering and trafficking (of people, drugs, weapons and illicit material). Investigation into the September 11, 2001 terrorist attack in the United States of America revealed that the perpetrators used fraudulent identification documents to board the ill-fated planes. A number of banks in East Africa have in the recent past lost substantial amounts of their customers' cash to fraudsters (Mumo, 2012). Law enforcement agencies have not been spared either by this new wave of crime. In January 2013, a man was arrested in Kenya for having successfully imposed himself as an assistant commissioner of the Kenyan police for more than five years (Gitonga, 2013). These examples show that the problem of identity fraud is huge and is affecting many sectors of the economy.

Identity fraud involves the use of false identifiers, false identification documents or a stolen identity to commit a crime. Normally, the intention of the fraudster is to gain money, goods, services, or avoid obligation. Though identity fraud has been in existence for a long time, its academic research started to pick up after the events of September 11, 2001. Research papers have been written from a variety of academic disciplines including information systems, computer science, law, accounting and finance. However, there is no evidence of the existence of a comprehensive academic literature review on the subject. Such a review is needed to guide future researchers in selecting appropriate research topics and relevant journals to publish their papers. This would aid in furthering the course of combating identity fraud.

The purpose of this paper is to survey literature on identity fraud and identify gaps in coverage and methodology that offer opportunity for future research.

The objectives are to:-

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

1) Identify academic literature that was published between 2002 and 2012 on identity fraud.
2) Examine the issues, trends and methods discussed in identity fraud literature.
3) Provide potential areas of future research on identity fraud.

Specifically, the paper addresses the following research questions:

1) How much academic literature on identity fraud was published from 2002 to 2012?
2) What are the issues discussed in identity fraud literature?
3) What are the trends in identity fraud research?
4) How is identity fraud research carried out?

It is hoped that the answers to these questions will add to the body of existing knowledge on identity fraud and provide directions for future research. We have structured the rest of the paper as follows: In Section 2, we describe our research methodology. In Section 3, we present results, which are answers to the research questions. In Section 4, we discuss the implications of the results and provide a conclusion in Section 5 together with a discussion on potential directions for further research.

METHODOLOGY

This study was undertaken as a systematic literature review based on the guidelines as proposed by Kitchenham(2004). In this method, a review protocol is developed to guide in searching and selecting relevant studies in addition to extracting data to answer pre-defined questions. The scope of the review was limited to the time frame of 2002-2012 because we believe that this time frame provides a fair representation of existing research on identity fraud. Electronic libraries were chosen as data sources. This was informed by the fact that academic literature on identity fraud is fairly current, and would be expected to have been published digitally. Digital libraries containing scientific, engineering and technology publications were chosen in consultation and with the help of Internet and library experts. Results yielded four electronic databases (1) Science Direct, (2) Scopus, (3) IEEE Xplore and (4) Lista (EBSCO).

In each electronic database, publications were searched using the search strings *"identity fraud", "identity theft" and "identity crime".* Articles published between 2002 and 2012 were defined in a search query. The search query was only applied to article abstracts, titles and keywords so as to minimize the chance of retrieving irrelevant publications. This means that an article is selected as a candidate for review if the abstract or title or keyword(s) contains the defined search string.

The articles retrieved were then uploaded to Endnote bibliographic software. With the assistance of this software, duplicate records were located and removed. An inclusion and exclusion criteria was developed to aid in filtering out the relevant publications. Those included for the review had to be written in English, formed part of original work, published between January 1st 2002 and December 31st 2012 and available in Science Citation Index Expanded (SCIE) or Engineering Index (EI) journals. The excluded publications were masters' theses, doctoral dissertations, news reports, textbooks, duplicates, and those without authors or abstracts.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

A total of 509 publications were retrieved and evaluated against the inclusion and exclusion criteria. The evaluation produced 121 articles which were then used as the sample of study.

RESULTS

This study reviewed academic literature on identity fraud. The study was motivated by a growing trend in identity fraud perpetration and a lack of a reliable source of information on the crime for both researchers and practitioners. Data collected was analyzed using qualitative and quantitative techniques. This section presents the analysis of the results.

The first objective of the study was to identify academic literature that was published between 2002 and 2012 on identity fraud. To achieve this objective, we searched relevant articles from the four (4) digital libraries. Data was collected under the question: *How much academic literature on identity fraud was published from 2002 to 2012?* The results are presented in Table 1, Table 2 and Fig. 1.
Table 1: lists the total number of articles retrieved from each digital library and those that were selected for the study. Though the Scopus database had the most retrieved articles, only 16.9% qualified for inclusion in the study. Lista (EBSCO) on the other hand, had the least number of the retrieved articles as well as the least number of selected ones (i.e. 5%). Science Direct and IEEE Xplore produced the most relevant publications from those retrieved with a selection of 52.7% and 45.7% respectively.

Table 1

Digital Library	Articles Retrieved	Articles Selected	Percentage Selected
Science Direct	93	49	52.7%
Scopus	302	51	16.9%
IEEE Xplore	35	16	45.7%
Lista (EBSCO)	79	4	5%
Total	**509**	**120**	**23.6%**

Table1: Number of Retrieved and Selected Articles

Table 2 lists the journals that published two or more articles. These journals comprised 22.2% of the total number of journals. The Journal of *Computer Fraud and Security* had the highest number of selected articles.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

Table 2

Journal	Citation	No. of Articles
Computer Fraud and Security	EI	19
Network Security	EI	8
Security & Privacy, IEEE	SCIE	8
Biometric Technology Today	EI	7
Card Technology Today	EI	6
Computers and Security	EI	3
Computer	SCIE	3
Engineering and Technology	EI	3
Information Security Journal	EI	3
Spectrum, IEEE	SCIE	3
Information Security Technical Report	EI	2
Journal of Computer Security	EI	2

Table 2: Journals publishing three or more articles on identity fraud

Fig. 1: presents the distribution of articles by year from 2002 to 2012. It shows that there has been an incremental production of articles on identity fraud over the 11-year period.

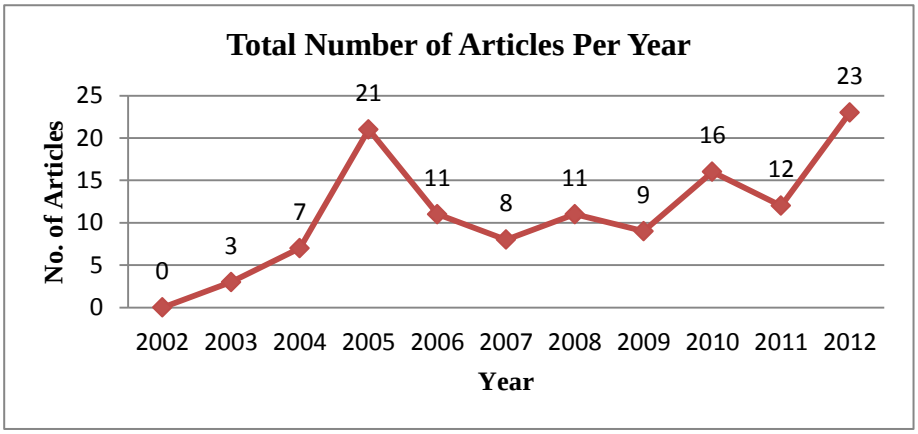

Fig. 1: Distribution of Articles by Year

Issues, Trends and Methods

The second objective of the study was to examine the issues, trends and methods discussed in identity fraud literature. To achieve this objective, we categorized the literature according to themes through a content-oriented analysis.

Issues

In this category, data was collected under the question: *What are the issues being discussed in identity fraud literature?* The results are presented under the following thematic areas; (*i) Technical Issues (ii) Policy and Legal Issues (iii) Target Sectors*. The details are presented in Table 3.

Technical Issues

These issues address identity fraud from an information technology perspective. They look at *what* is understood by identity fraud, *how* the fraud is perpetrated and *how* it can be detected, prevented and investigated.

(i) Definition

A few research papers have attempted to define the term "identity fraud". According to Hinde(2005),identity fraud involves the stealing of financial or other private information (identity theft), or using totally invented information to make purchases or gain access to financial accounts. Others like Pemble(2008) argue that personal identification information cannot be stolen since the original owner of the information still has it in its original format.

(ii) Perpetration Methods

There are different techniques used to perpetrate identity fraud in both the online and offline environments. Some of these techniques include phishing (Aburrous, Hossain, Dahal, & Thabtah, 2010; McCarty, 2003; Eisen, 2009), dumpster diving (Jones, 2005), forgery (Chollet et al., 2012) and exploitation of human weaknesses (Bang, Lee, Bae, & Ahn, 2012; S. M. Furnell, 2010) . Phishing, which is a form of electronic identity theft in which a combination of social and technical techniques is used to trick a user into revealing confidential information(Aburrous et al., 2010), has been studied the most.

(iii) Detection and Prevention

Several papers have suggested different ways of detecting and preventing identity fraud. Most of the detection models such as (Becker, Volinsky, & Wilks, 2010; Dong, Clark, & Jacob, 2010) have been proposed for online environment. Solutions to identity fraud range from technical like biometric, smart card and encryption to theoretical ones. The theoretical solutions which form the bigger part in the category address mainly the phishing problem.

(iv) Investigation

Other articles have attempted to uncover information about the perpetration of identity fraud. Forensic science techniques (Curran, Robinson, Peacocke, & Cassidy, 2010) have been incorporated intosuch

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

investigations which reveal the methods usedthereby assist practitioners improve the effectiveness of solutions to identity fraud.Fig. 2 presents the distribution of articles by technical issues.

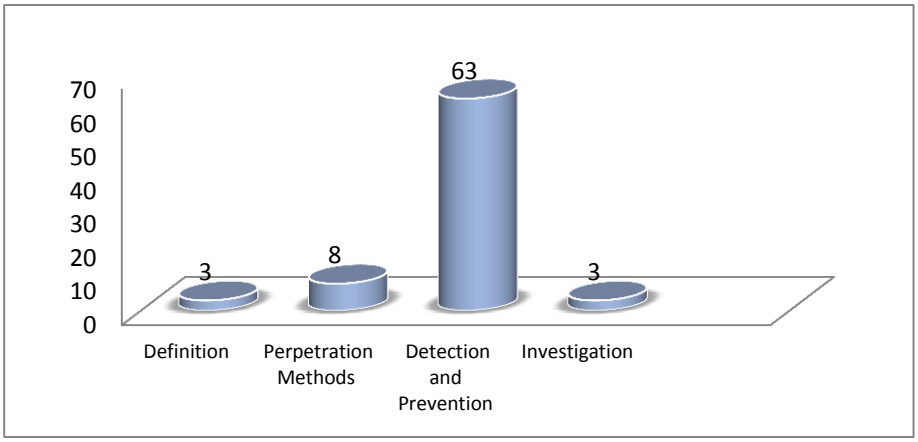

Fig. 2: Distribution of Articles by Technical Issues

Policy and Legal Issues

These issues revolve around how governments and the private sector have or should formulate policies on identity fraud. Some countries faced resistance from the public when trying to legislate on policies aimed at curbing the vice (Guizzo, 2006; Whitley & Hosein, 2008). Those opposed to the legislature argue that the proposed human identification solutions would infringe on their privacy.

Target Sectors

From the 34 papers that discussed identity fraud in specific sectors, 21 (61.8%) concentrated on the financial sector. Such sectors as security which are of current concern were not well represented in the research. Fig. 3 presents distribution of articles by target sector.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

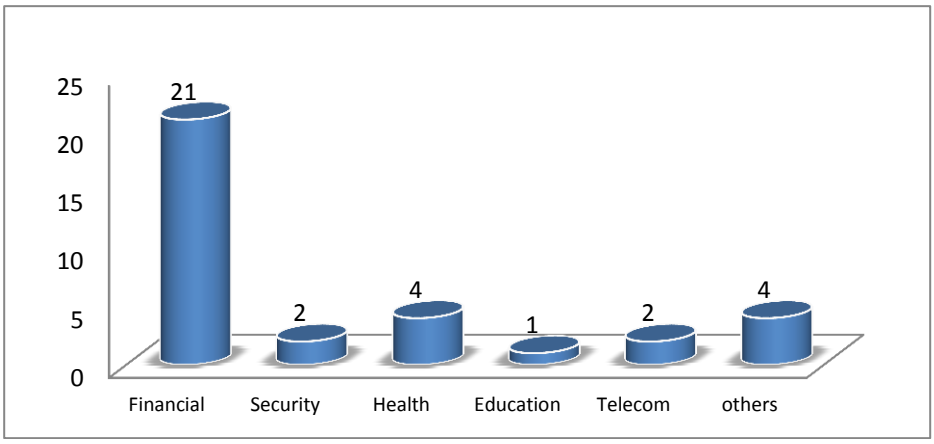

Fig. 3: Distribution of Articles by Target Sector

Trends

In this category, data was collected under the question: *What are the trends in identity fraud literature?* According to reports from The Federal Trade Commission (FTC), there has been a continuous growth of identity theft and fraud. The number of identity theft cases were found to be higher in regions with large populations in the United States of America, (Koong, Liu, Bai, & Lin, 2008). Phishing attacks in particular rose consistently (Stephen Hinde, 2004), a trend which is still being maintained to date. The trend towards cloud based-computing is expected to increase online attacks and hence identity fraud.

Type of Research

This part answered the research question: *How is identity fraud research carried out?* We looked at the research methods that were used by identity fraud researchers. The articles were categorized into survey, historical, observational and experimental types of research as defined by Mugenda and Mugenda(2003). Observational type of research was utilized by 51.7% of the studies followed by experimental with 25% and survey with 22.5%. Historical research was the least with 0.8% of studies using this method. The details are presented in Fig. 4 below.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

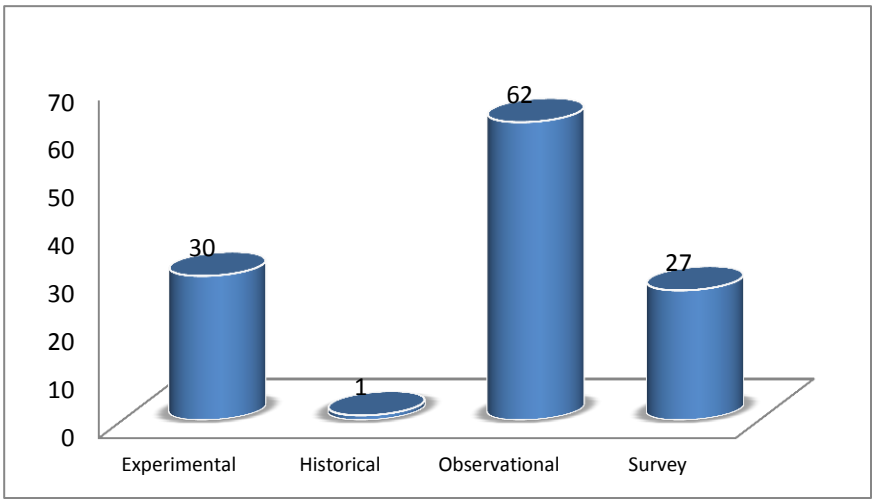

Fig. 4: Distribution of Articles by Type of Research

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

Table 3: Classification by themes

Theme	Sub-Theme	Specific Area	References
Technical Issues	Definition		(Pemble, 2008), (Steven Hinde, 2005), (Geer Jr & Conway, 2008)
	Perpetration Methods	*Phishing*	(Aburrous et al., 2010), (McCarty, 2003), (Eisen, 2009)
		Dumpster Diving	(Jones, 2005)
		Forgery	(Chollet et al., 2012)
		Human Factor	(Bang et al., 2012), (S. M. Furnell, 2010), (Keaney, 2009)
	Detection and Prevention	*Biometrics and Smartcards*	(Andrew B. J. Teoh, Kuan, & Lee, 2008), (Lu & Ali, 2010), (Grijpink, 2005), (Jain & Pankanti, 2006a), (Jain & Pankanti, 2006b), (Moore, 2006), (Morrison, 2007), (Napua, 2011), (Sagar, 2012), (Ajana, 2010), (Sood, 2011), (Arndt, 2005), (Aulich, 2005), (A. B. J. Teoh, Goh, & Ngo, 2006), (Cave, 2005), (V. Lee, 2008), (Ram & Gadepalli, 2007), (Weaver, 2006), (Xiao, 2007), (Ngugi, Kahn, & Tremaine, 2011), (Pawlewski & Jones, 2006)
		Encryption	(Bhargav-Spantzel, Squicciarini, & Bertino, 2006), (Goodrich, Tamassia, & Yao, 2008), (Nandakumar, Jain, & Pankanti, 2007), (Kozat, Vlachos, Lucchese, Van Herle, & Yu, 2009), (Nagy, Nagy, & Akl, 2010), (Dolev & Kopeetsky, 2012), (Edge & Falcone Sampaio, 2009)
		Theoretical	(Choi & Lee, 2012), (Liang, Lu, Chen, Lin, & Shen, 2011), (Konidala et al., 2012), (Lenzini, Bargh, & Hulsebosch, 2008), (Pantel, Philpot, & Hovy, 2005), (Phiri, Zhao, & Mbale, 2011), (Phiri, Zhao, Zhu, & Mbale, 2011), (Vu, Chambers, Creekmur, Cho, & Proctor, 2010), (Vural & Venter, 2012), (Lai, Li, & Hsieh, 2012), (Feher, Elovici, Moskovitch, Rokach, & Schclar, 2012), (Akram, Misbahuddin, & Varaprasad, 2012), (Gupta & Pieprzyk, 2011), (Han, Cao, Bertino, & Yong, 2012), (Hinde, 2003), (Salem & Stolfo, 2012), (Huang, Qian, & Wang, 2012), (Kuan-Ta, Jau-Yuan, Chun-Rong, & Chu-Song, 2009), (Gerdes Jr, Kalvenes, & Huang, 2009), (Ivanov, Yu, & Baras, 2010), (Kirda & Kruegel, 2006), (Walton Cb, 2005), (Wenjie, Yufei, & Archer, 2006), (Dyhouse, 2009), (Kemp, 2010), (B. Dwan, 2005), (Greamo & Ghosh, 2011), (Dong et al., 2010), (Shareef & Kumar, 2012), (Zhenhai et al., 2012), (Sullivan, 2005), (Canfora & Visaggio, 2012), (Hallam-Baker, 2005),(Becker et al., 2010)
	Investigation		(McLemore, Hodges, & Wyman, 2011), (Knight, 2010), (Curran et al., 2010)
Policy and Legal Issues			(Loo, 2009), (Guizzo, 2006), (Hunter, 2005a), (Hunter, 2005b), (Seven Hinde, 2004), (Elbirt, 2005a), (Elbirt, 2005b), (Schneider, 2007), (Whitley & Hosein, 2008)
Target Sectors	*Financial*		(Granova & Eloff, 2004),(Aburrous et al., 2010), (Berni Dwan, 2004), (Hallam-Baker, 2005), (Gupta & Pieprzyk, 2011), (Hinde, 2003), (Harald, 2008), (Steven Hinde, 2005), (Stephen Hinde, 2005), (Hunter, 2005a), (Jain & Pankanti, 2006a), (Konidala et al., 2012), (J.-E. R. Lee, Rao, Nass, Forssell, & John, 2012), (Lord, 2012), (Meadowcroft, 2005), (Meadowcroft, 2008), (Moore, 2006), (Gitonga, 2013), (Porter, 2004), (Scheflen, 2005), (Shareef & Kumar, 2012)
			(Ram & Gadepalli, 2007), (Sagar, 2012)
	Security		(Ivanov et al., 2010), (Jones, 2005), (McLemore et al., 2011), (Napua, 2011)
	Health		(Jones, 2005)
	Education		(Ghosh, 2010), (Becker et al., 2010)
	Telecommunication		(Sangani, 2011), (Jones, 2005), (S. Furnell & Botha, 2011), (William Newk-Fon Hey, Peter, & John, 2010)
	Others		
Trends			(Lane & Sui, 2010), (Stephen Hinde, 2004), (Koong et al., 2008)
Others			(J.-E. R. Lee et al., 2012), (Altshuler, Aharony, Pentland, Elovici, & Cebrian, 2011), (Caloyannides, 2004), (Berni Dwan, 2004), (Geer Jr & Conway, 2008), (Stephen Hinde, 2005), (Holz, 2005), (Lord, 2012), (Mansfield-Devine, 2010), (Philpott, 2006), (Porter, 2004), (Renaud & Goucher, 2012), (Rozenberg, 2012), (Voice, 2005), (Granova & Eloff, 2004), (Berghel, 2012), (Harald, 2008), (Meadowcroft, 2005), (Meadowcroft, 2008), (Pollard, 2005), (Sangani, 2011), (Scheflen, 2005), (Wilbanks, 2007), (Williamson, 2008), (Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2004), (S. Furnell, 2007), (S. Furnell & Botha, 2011), (Moir & Weir, 2009), (Tan & Aguilar, 2012), (Keaney, 2009), (William Newk-Fon Hey et al., 2010), (Workman & Gathegi, 2007)

Table 4

Type of Research	References
Experimental	(A. B. J. Teoh et al., 2006), (Zhenhai et al., 2012), (J.-E. R. Lee et al., 2012), (Choi & Lee, 2012), (Liang et al., 2011), (Konidala et al., 2012), (Lenzini et al., 2008), (Pantel et al., 2005), (Phiri, Zhao, & Mbale, 2011), (Phiri, Zhao, Zhu, et al., 2011), (Andrew B. J. Teoh et al., 2008), (Vu et al., 2010), (Vural & Venter, 2012), (Lai et al., 2012), (Feher et al., 2012), (Akram et al., 2012), (Bhargav-Spantzel et al., 2006), (Goodrich et al., 2008), (Gupta & Pieprzyk, 2011), (Han et al., 2012), (Hinde, 2003), (Lu & Ali, 2010), (Nandakumar et al., 2007), (Salem & Stolfo, 2012), (Huang et al., 2012), (Kozat et al., 2009), (Kuan-Ta et al., 2009), (Aburrous et al., 2010), (Jones, 2005), (Lane & Sui, 2010)
Historical	(Becker et al., 2010)
Observational	(Pemble, 2008), (McLemore et al., 2011), (Knight, 2010), (Altshuler et al., 2011), (Loo, 2009), (Caloyannides, 2004), (B. Dwan, 2005), (Geer Jr & Conway, 2008), (Ghosh, 2010), (Guizzo, 2006), (Hallam-Baker, 2005), (Steven Hinde, 2005), (Holz, 2005), (Hunter, 2005a), (Hunter, 2005b), (Lord, 2012), (Mansfield-Devine, 2010), (Philpott, 2006), (Porter, 2004), (Renaud & Goucher, 2012), (Rozenberg, 2012), (Sullivan, 2005), (Voice, 2005), (Granova & Eloff, 2004), (Stephen Hinde, 2004), (Berghel, 2012), (Cave, 2005), (Elbirt, 2005a), (Elbirt, 2005b), (Harald, 2008), (V. Lee, 2008), (Meadowcroft, 2005), (Meadowcroft, 2008), (Pollard, 2005), (Ram & Gadepalli, 2007), (Sangani, 2011), (Scheflen, 2005), (Schneider, 2007), (Weaver, 2006), (Wilbanks, 2007), (Williamson, 2008), (Xiao, 2007), (Whitley & Hosein, 2008), (Nagy et al., 2010), (Gerdes Jr et al., 2009), (Grijpink, 2005), (Ivanov et al., 2010), (Kirda & Kruegel, 2006), (Walton Cb, 2005), (Wenjie et al., 2006), (Dyhouse, 2009), (Jain & Pankanti, 2006a), (Jain & Pankanti, 2006b), (Kemp, 2010), (Moore, 2006), (Morrison, 2007), (Napua, 2011), (Sagar, 2012), (Berni Dwan, 2004), (Bang et al., 2012), (McCarty, 2003) , (Geer Jr & Conway, 2008)
Survey	(Stephen Hinde, 2005), (Curran et al., 2010), (Sharp et al., 2004), (Canfora & Visaggio, 2012), (S. Furnell, 2007), (S. Furnell & Botha, 2011), (S. M. Furnell, 2010), (Moir & Weir, 2009), (Tan & Aguilar, 2012), (Keaney, 2009), (Ngugi et al., 2011), (Pawlewski & Jones, 2006), (William Newk-Fon Hey et al., 2010), (Workman & Gathegi, 2007), (Ajana, 2010), (Dolev & Kopeetsky, 2012), (Edge & Falcone Sampaio, 2009), (Greamo & Ghosh, 2011), (Sood, 2011), (Arndt, 2005), (Aulich, 2005), (Dong et al., 2010), (Shareef & Kumar, 2012), (Eisen, 2009), (Chollet et al., 2012), (Seven Hinde, 2004), (Koong et al., 2008)

Table 4: Classification by Type of Research

DISCUSSION

The first objective of this study was to identify academic literature on identity fraud that was published between 2002 and 2012. Overall, 120 relevant articles were identified from the digital libraries as shown in Table 1. The results reveal that much has been written on identity fraud though a great percentage (76.4%) was not relevant to the study. This lack of relevance could be a result of immaturity of research in the field which may have led researchers publish their work in any journal they came across irrespective of whether the journal is recognized or not. The number of articles published between 2002 and 2005 had an exponential growth. Much of the discussion during this period was in the context of the United States of America and the United Kingdom. This can be attributed to the development of e-commerce applications in those countries and the terrorist attacks of September 11, 2001.The highest number of identify fraud publications were in the year 2012 that could be explained by the rise in online activities such as social networking, e-commerce, e-mailing and subsequent threats such as phishing may explain this high number.

The second objective was to examine the issues, trends and methods discussed in identity fraud literature. This objective was addressed through a content-oriented analysis of literature.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

In the technical issues category, the definition of identity fraud seems to suggest that this crime is carried out for financial reasons only, which may not be the case. Consequently, identity fraud could be defined as "the use of false identifiers, false identification documents or a stolen identity to commit a crime". The definition covers other crimes like terrorism, drug and weapon trafficking, employment fraud, academic certificate forgeries and other crimes to identity fraud. The methods used by criminals to carry out identity fraud were majorly discussed as they relate to the online environment. Offline methods may have been neglected because majority of these studies were done in the context of developed nations, where automation has been done in virtually all sectors. Software applications have been developed to detect online identity fraud, though they have not been as effective as anticipated. Though technical solutions for preventing identity fraud such as biometrics, smartcards and encryption helped in reducing the crime, they were also vulnerable to new methods of attack.

The policy and legal issues address identity fraud from the perspective of the political class (Guizzo, 2006; Whitley & Hosein, 2008). The voice of the professionals has not been clear in the academic literature. Most governments have been unable to balance privacy and security issues in their endeavour to introduce national identification systems to curb identity fraud and other related crimes. The financial sector received more research attention than the other sectors. This may have been due to the growth of online financial solutions. Other important sectors like security, health, education have not received much attention.

The rising trend in identity fraud was discussed with regard to identity theft. Identity fraud also involves the use of fictitious identities or giving identity deception details when committing a crime. Trends in terms of fictitious identities or identity deception details are lacking.

Finally, researchers have employed different methods to undertake their research. Historical research has not been fully exploited. More historical studies should be undertaken on identity fraud because enough background information on the subject is lacking.

Further research

The ever growing prevalence of identity fraud, complexity and adverse impacts on the global security and economy necessitates advanced research in this field. Some of the areas identified are:

- The possibility of developing a Global Identification System.While one country can implement a very secure identification system, the integrity of that system is affected by the integrity of other external systems. Could a global identification system be the solution?
- Models, theories, frameworks, methods, techniques and tools for combating identity fraud should be developed.
- Identity fraud should be studied in the offline environment, especially in developing countries where many systems are still operated manually.
- The methods and ways used by criminals to perpetrate identity fraud have not been studied exhaustively. Empirical studies need to be carried out to fill these gaps.
- National and global security implications of identity fraud need to be thoroughly investigated.
- Policy and legal frameworks that deal with identity fraud and address security and privacy issues may need to be developed.
- Organizations/bodies/persons concerned with issues of identity fraud should be investigated to identify their roles, composition and challenges in relation to identity fraud.

CONCLUSION

This study reviewed literature on identity fraud that was published between 2002 and 2012. It was intended to identify gaps in coverage and methodology that offer opportunity for future research. This was in relation to a growing trend in identity fraud perpetration and a lack of a reliable source of information on the crime for both researchers and practitioners. The study specifically sought to 1) identify academic literature that was published between 2002 and 2012 on identity fraud, 2) examine the issues, trends and methods discussed in identity fraud literature and 3) provide potential areas of future research on identity fraud. The study established that a lot of research has been done on identity fraud but there is scarcity of relevant quality research. Identity fraud has not been understood holistically and has mainly been studied in the context of developed countries and in online environment. The public and private sectors have not partnered to address policy and legal issues with regard to identity fraud. In view of these findings, the study concludes that identity fraud is an important21st century research topic that needs to be pursued from a variety of perspectives based on multiple academic disciplines.

REFERENCE

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Cognitive Computation, 2*(3), 242-253.

Ajana, B. (2010). Recombinant identities: Biometrics and narrative bioethics. *Journal of Bioethical Inquiry, 7*(2), 237-258.

Akram, S., Misbahuddin, M., & Varaprasad, G. (2012). A usable and secure two-factor authentication scheme. *Information Security Journal, 21*(4), 169-182.

Altshuler, Y., Aharony, N., Pentland, A., Elovici, Y., & Cebrian, M. (2011). Stealing reality: When criminals become data scientists (or vice versa). *IEEE Intelligent Systems, 26*(6), 22-30.

Arndt, C. (2005). The loss of privacy and identity. *Biometric Technology Today, 13*(8), 6-7. doi: http://dx.doi.org/10.1016/S0969-4765(05)70386-6

Aulich, T. (2005). Putting into practice a privacy code. *Biometric Technology Today, 13*(10), 8-9. doi: http://dx.doi.org/10.1016/S0969-4765(05)70412-4

Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. International *Journal of Information Management, 32*(5), 409-418. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2012.01.001

Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud detection in telecommunications: History and lessons learned. *Technometrics, 52*(1), 20-33.

Berghel, H. (2012). Identity theft and financial fraud: Some strangeness in the proportions. *Computer, 45*(1), 86-89.

Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2006). Establishing and protecting digital identity in federation systems. *Journal of Computer Security, 1*4(3), 269-300.

Caloyannides, M. A. (2004). The cost of convenience: a faustian deal [computer security]. *IEE Security & Privacy, 2*(2), 84-87. doi: 10.1109/msecp.2004.1281255

Canfora, G., & Visaggio, C. A. (2012). Managing trust in social networks. *Information Security Journal, 21*(4), 206-215.

Cave, J. (2005). An economics view of biometrics. *Biometric Technology Today, 13*(5), 8-11. doi: http://dx.doi.org/10.1016/S0969-4765(05)70328-3

Choi, H., & Lee, H. (2012). Identifying botnets by capturing group activities in DNS traffic. *Computer Networks, 56*(1), 20-33. doi: http://dx.doi.org/10.1016/j.comnet.2011.07.018

Chollet, G., Perrot, P., Karam, W., Mokbel, C., Kanade, S., & Petrovska-Delacrétaz, D. (2012). Identities, forgeries and disguises. *International Journal of Information Technology and Management, 11*(1-2), 138-152.

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile phone forensic analysis. *International Journal of Digital Crime and Forensics, 2*(3), 15-27.

Dolev, S., & Kopeetsky, M. (2012). Anonymous transactions in computer networks. *ACM Transactions on Autonomous and Adaptive Systems, 7*(2).

Dong, X., Clark, J. A., & Jacob, J. L. (2010). Defending the weakest link: Phishing websites detection by analysing user behaviours. *Telecommunication Systems, 45*(2-3), 215-226.

Dwan, B. (2004). Identity theft. *Computer Fraud & Security, 2004*(4), 14-17. doi: http://dx.doi.org/10.1016/S1361-3723(04)00055-7

Dwan, B. (2005). Pervasive spyware. *Network Security, 2005*(1), 19.

Dyhouse, T. (2009). Analysis: A unified framework for IT security. *Engineering & Technology, 4*(11), 58-58.

Edge, M. E., & Falcone Sampaio, P. R. (2009). A survey of signature based methods for financial fraud detection. *Computers & Security, 28*(6), 381-394. doi: http://dx.doi.org/10.1016/j.cose.2009.02.001

Eisen, O. (2009). In-session phishing and knowing your enemy. *Network Security, 2009*(3), 8-11. doi: http://dx.doi.org/10.1016/S1353-4858(09)70027-3

Elbirt, A. J. (2005a). Living with technology: Who are you? How to protect against identity theft. *IEEE Technology and Society Magazine, 24*(2), 5-8.

Elbirt, A. J. (2005b). Who are you? How to protect against identity theft. *IEEE Technology and Society Magazine, 24*(2), 5-8. doi: 10.1109/mtas.2005.1442375

Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., & Schclar, A. (2012). User identity verification via mouse dynamics. *Information Sciences, 201*, 19-36. doi: http://dx.doi.org/10.1016/j.ins.2012.02.066

Furnell, S. (2007). Identity impairment: The problems facing victims of identity fraud. *Computer Fraud & Security, 2007*(12), 6-11. doi: http://dx.doi.org/10.1016/S1361-3723(07)70168-9

Furnell, S., & Botha, R. A. (2011). Social networks – access all areas? *Computer Fraud & Security, 2011*(5), 14-19. doi: http://dx.doi.org/10.1016/S1361-3723(11)70052-5

Furnell, S. M. (2010). Online identity: Giving it all away? *Information Security Technical Report, 15*(2), 42-46. doi: http://dx.doi.org/10.1016/j.istr.2010.09.002

Geer Jr, D. E., & Conway, D. G. (2008). Beware the IDs of March. *IEEE Security and Privacy, 6*(2), 87.

Gerdes Jr, J. H., Kalvenes, J., & Huang, C. T. (2009). Multi-dimensional credentialing using veiled certificates: Protecting privacy in the face of regulatory reporting requirements. *Computers and Security, 2*8(5), 248-259.

Ghosh, M. (2010). Mobile ID fraud: the downside of mobile growth. *Computer Fraud & Security, 2010*(12), 8-13. doi: http://dx.doi.org/10.1016/S1361-3723(10)70155-X

Gitonga, A. (2013, January 4 2013). Imposter PPO was a tout, News, *Standard Digital*. Retrieved from http://www.standardmedia.co.ke/?articleID=2000074171

Goodrich, M. T., Tamassia, R., & Yao, D. (2008). Notarized federated ID management and authentication. *Journal of Computer Security, 16*(4), 399-418.

Granova, A., & Eloff, J. H. P. (2004). Online banking and identity theft: who carries the risk? *Computer Fraud & Security, 2004*(11), 7-11. doi: http://dx.doi.org/10.1016/S1361-3723(04)00134-4

Greamo, C., & Ghosh, A. (2011). Sandboxing and virtualization: Modern tools for combating malware. *IEEE Security and Privacy,* 9(2), 79-82.

Grijpink, J. (2005). Biometrics and identity fraud protection: Two barriers to realizing the benefits of biometrics - A chain perspective on biometrics, and identity fraud - Part II. *Computer Law and Security Report, 21*(3), 249-256.

Guizzo, E. (2006). Britain's identity crisis [biometric ID cards]. *Spectrum, IEEE, 43*(1), 42-43. doi: 10.1109/MSPEC.2006.1572352

Gupta, G., & Pieprzyk, J. (2011). Socio-technological phishing prevention. *Information Security Technical Report, 16*(2), 67-73. doi: http://dx.doi.org/10.1016/j.istr.2011.09.003

Hallam-Baker, P. (2005). Prevention strategies for the next wave of cyber crime. *Network Security, 2005*(10), 12-15. doi: http://dx.doi.org/10.1016/S1353-4858(05)70291-9

Han, W., Cao, Y., Bertino, E., & Yong, J. (2012). Using automated individual white-list to protect web digital identities. Expert Systems with Applications, 39(15), 11861-11869. doi: http://dx.doi.org/10.1016/j.eswa.2012.02.020

Harald, B. (2008). Banking on identity. *Card Technology Today, 20*(3), 9. doi: http://dx.doi.org/10.1016/S0965-2590(08)70075-6

Hinde, S. (2003). Careless about privacy. *Computers and Security, 22*(4), 284-288.

Hinde, S. (2004). ID theft: the US legal fight back. *Computer Fraud & Security, 2004*(10), 7-9. doi: http://dx.doi.org/10.1016/S1361-3723(04)00121-6

Hinde, S. (2004). Identity theft: the fight. *Computer Fraud & Security, 2004*(9), 6-7. doi: http://dx.doi.org/10.1016/S1361-3723(04)00110-1

Hinde, S. (2005). Identity theft & fraud. *Computer Fraud & Security, 2005*(6), 18-20. doi: http://dx.doi.org/10.1016/S1361-3723(05)70223-2

Hinde, S. (2005). Identity theft: theft, loss and giveaways. *Computer Fraud & Security, 2005*(5), 18-20. doi: http://dx.doi.org/10.1016/S1361-3723(05)70215-3

Holz, T. (2005). A short visit to the bot zoo [malicious bots software]. *IEEE Security & Privacy, 3*(3), 76-79. doi: 10.1109/msp.2005.58

Huang, H., Qian, L., & Wang, Y. (2012). A SVM-based technique to detect phishing URLs. *Information Technology Journal, 11*(7), 921-925.

Hunter, P. (2005a). CardSystems: four million hack – under the spotlight. *Computer Fraud & Security, 2005*(11), 8-9. doi: http://dx.doi.org/10.1016/S1361-3723(05)70274-8

Hunter, P. (2005b). ChoicePoint saga repercussions: Not an information security breach? *Computer Fraud & Security, 2005*(4), 5-7. doi: http://dx.doi.org/10.1016/S1361-3723(05)70198-6

Ivanov, V. I., Yu, P. L., & Baras, J. S. (2010). Securing the communication of medical information using local biometric authentication and commercial wireless links. *Health Informatics Journal, 16*(3), 211-223. doi: 10.1177/1460458210377482

Jain, A. K., & Pankanti, S. (2006b). A touch of money [biometric authentication systems]. *IEEE Spectrum, 43*(7), 22-27. doi: 10.1109/mspec.2006.1653001

Jones, A. (2005). How much information do organizations throw away? *Computer Fraud & Security, 2005*(3), 4-9. doi: http://dx.doi.org/10.1016/S1361-3723(05)70170-6

Keaney, A. (2009). Identity theft and privacy - Consumer awareness in Ireland. *International Journal of Networking and Virtual Organisations,* 6(6), 620-633.

Kemp, G. (2010). Fighting public sector fraud in the 21st century. *Computer Fraud and Security, 2010*(11), 16-18.

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. *Computer Journal, 49*(5), 554-561.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews Joint Technical Report.

Knight, E. (2010). Investigating digital fingerprints: advanced log analysis. Network Security, 2010(10), 17-20. doi: http://dx.doi.org/10.1016/S1353-4858(10)70127-6

Konidala, D. M., Dwijaksara, M. H., Kim, K., Lee, D., Lee, B., Kim, D., & Kim, S. (2012). Resuscitating privacy-preserving mobile payment with customer in complete control. Personal and *Ubiquitous Computing, 16*(6), 643-654.

Koong, K. S., Liu, L. C., Bai, S., & Lin, B. (2008). Identity theft in the USA: Evidence from 2002 to 2006. *International Journal of Mobile Communications,* 6(2), 199-216.

Kozat, S. S., Vlachos, M., Lucchese, C., Van Herle, H., & Yu, P. S. (2009). Embedding and retrieving private metadata in electrocardiograms. *Journal of Medical Systems, 33*(4), 241-259.

Kuan-Ta, C., Jau-Yuan, C., Chun-Rong, H., & Chu-Song, C. (2009). Fighting phishing with discriminative keypoint features.*IEEE Internet Computing*, 13(3), 56-63. doi: 10.1109/mic.2009.59

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353-363. doi: http://dx.doi.org/10.1016/j.dss.2011.09.002

Lane, G. W., & Sui, D. Z. (2010). Geographies of identity theft in the U.S.: Understanding spatial and demographic patterns, 2002-2006. *GeoJournal, 75*(1), 43-55.

Lee, J.-E. R., Rao, S., Nass, C., Forssell, K., & John, J. M. (2012). When do online shoppers appreciate security enhancement efforts? Effects of financial risk and security level on evaluations of customer authentication. *International Journal of Human-Computer Studies, 70*(5), 364-376. doi: http://dx.doi.org/10.1016/j.ijhcs.2011.12.002

Lee, V. (2008). Biometrics and identity fraud. *Biometric Technology Today, 16*(2), 7-11. doi: http://dx.doi.org/10.1016/S0969-4765(08)70059-6

Lenzini, G., Bargh, M. S., & Hulsebosch, B. (2008). Trust-enhanced security in location-based adaptive authentication. Electronic Notes in *Theoretical Computer Science, 197*(2), 105-119. doi: http://dx.doi.org/10.1016/j.entcs.2007.12.020

Liang, X., Lu, R., Chen, L., Lin, X., & Shen, X. (2011). PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks. Journal of *Communications and Networks, 13*(2), 102-112.

Loo, A. (2009). Technical opinion: Security threats of smart phones and Bluetooth. *Communications of the ACM, 52*(3), 150-152.

Lord, J. (2012). The case for strong identities. *Computer Fraud & Security, 2012*(5), 16-17. doi: http://dx.doi.org/10.1016/S1361-3723(12)70043-X

Lu, H. K., & Ali, A. M. (2010). Making smart cards truly portable. *IEEE Security & Privacy, 8*(2), 28-34. doi: 10.1109/msp.2010.56.

Mansfield-Devine, S. (2010). The perils of sharing. *Network Security, 2010*(1), 11-13. doi: http://dx.doi.org/10.1016/S1353-4858(10)70015-5

McCarty, B. (2003). Automated identity theft. *IEEE Security & Privacy, 1*(5), 89-92. doi: 10.1109/msecp.2003.1236244

McLemore, J., Hodges, W., & Wyman, A. (2011). Impact of identity theft on methods of identification. *American Journal of Forensic Medicine and Pathology, 32*(2), 143-145.

Meadowcroft, P. (2005). Combating cardholder not present fraud. *Card Technology Today, 17*(7–8), 12-13. doi: http://dx.doi.org/10.1016/S0965-2590(05)70350-9

Meadowcroft, P. (2008). Card fraud – will PCI-DSS have the desired impact? *Card Technology Today, 20*(3), 10-11. doi: http://dx.doi.org/10.1016/S0965-2590(08)70076-8

Moir, I., & Weir, G. R. S. (2009). Contact centres and identity theft. *International Journal of Electronic Security and Digital Forensics,* 2(1), 92-100.

Moore, A.-M. (2006). A smart solution for biometrics. *Card Technology Today, 18*(3), 9. doi: http://dx.doi.org/10.1016/S0965-2590(06)70466-2

Morrison, R. (2007). Commentary: Multi-factor identification and authentication. Information *Systems Management, 24*(4), 331-332. doi: 10.1080/10580530701586052

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches.* Nairobi: ACTS Press.

Mumo, M. (2012, July 31, 2012). East African banks lose US$48.3 million to fraud, *Daily Nation*.

Nagy, N., Nagy, M., & Akl, S. G. (2010). Hypercomputation in a cryptographic setting: Solving the identity theft problem using quantum memories. *International Journal of Unconventional Computing, 6*(5), 375-398.

Nandakumar, K., Jain, A. K., & Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security,* 2(4), 744-757.

Napua, J. (2011). Growth of biometric technology in self-service situations. *Fujitsu Scientific and Technical Journal, 47*(1), 68-74.

Ngugi, B., Kahn, B. K., & Tremaine, M. (2011). Typing biometrics: Impact of human learning on performance quality. *Journal of Data and Information Quality, 2*(2).

Pantel, P., Philpot, A., & Hovy, E. (2005). Data alignment and integration [US government]. *Computer, 38*(12), 43-50. doi: 10.1109/mc.2005.406

Pawlewski, M., & Jones, J. (2006). Speaker verification: Part 1. *Biometric Technology Today, 14*(6), 9-11. doi: http://dx.doi.org/10.1016/S0969-4765(06)70554-9

Pemble, M. (2008). Don't panic: taxonomy for identity theft. *Computer Fraud & Security, 2008*(7), 7-9. doi: http://dx.doi.org/10.1016/S1361-3723(08)70111-8

Philpott, A. (2006). Identity theft – dodging the own-goals. *Network Security, 2006*(1), 11-13. doi: http://dx.doi.org/10.1016/S1353-4858(06)70323-3

Phiri, J., Zhao, T. J., & Mbale, J. (2011). Identity attributes mining, metrics composition and information fusion implementation using fuzzy inference system. *Journal of Software, 6*(6), 1025-1033.

Phiri, J., Zhao, T. J., Zhu, C. H., & Mbale, J. (2011). Using artificial intelligence techniques to implement a multifactor authentication system. *International Journal of Computational Intelligence Systems, 4*(4), 420-430.

Pollard, C. (2005). Identity management – time to start playing your cards right. *Card Technology Today, 17*(11–12), 12-13. doi: http://dx.doi.org/10.1016/S0965-2590(05)70408-4

Porter, D. (2004). Identity fraud: the stealth threat to UK plc. *Computer Fraud & Security, 2004*(7), 4-6. doi: http://dx.doi.org/10.1016/S1361-3723(04)00086-7

Ram, J., & Gadepalli, M. (2007). The case for biometric passports in emerging markets. *Biometric Technology Today, 15*(3), 7-8. doi: http://dx.doi.org/10.1016/S0969-4765(07)70081-4

Renaud, K., & Goucher, W. (2012). Email passwords: Pushing on a latched door. *Computer Fraud and Security, 2012*(9), 16-19.

Rozenberg, Y. (2012). Challenges in PII data protection. *Computer Fraud & Security, 2012*(6), 5-9. doi: http://dx.doi.org/10.1016/S1361-3723(12)70061-1

Sagar, N. (2012). AFIS technology: driving the age of authentic impressions. *Biometric Technology Today, 2012*(1), 5-7. doi: http://dx.doi.org/10.1016/S0969-4765(12)70033-4

Salem, M. B., & Stolfo, S. J. (2012). A comparison of one-class bag-of-words user behavior modeling techniques for masquerade detection. *Security and Communication Networks, 5*(8), 863-872.

Sangani, K. (2011). Sony security laid bare. *Engineering and Technology, 6*(8), 74-77.

Scheflen, K. (2005). Ensuring security by managing identity. *Card Technology Today, 17*(6), 12-13. doi: http://dx.doi.org/10.1016/S0965-2590(05)70328-5

Schneider, F. B. (2007). Technology scapegoats and policy saviors.*IEEE Security & Privacy, 5*(5), 3-4. doi: 10.1109/msp.2007.124

Shareef, M. A., & Kumar, V. (2012). Prevent/control identity theft: Impact on trust and consumers' purchase intention in B2C EC. *Information Resources Management Journal, 25*(3), 30-60.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2004). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences, 49*(1), 131-136.

Sood, S. K. (2011). Secure dynamic identity-based authentication scheme using smart cards. *Information Security Journal, 20*(2), 67-77.

Sullivan, R. K. (2005). The case for federated identity. *Network Security, 2005*(9), 15-19. doi: http://dx.doi.org/10.1016/S1353-4858(05)70283-X

Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of Bluetooth security. *Information Management & Computer Security, 20*(5), 364-381. doi: 10.1108/09685221211286539

Teoh, A. B. J., Goh, A., & Ngo, D. C. L. (2006). Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 28*(12), 1882-1901.

Teoh, A. B. J., Kuan, Y. W., & Lee, S. (2008). Cancellable biometrics and annotations on BioHash. *Pattern Recognition, 41*(6), 2034-2044. doi: http://dx.doi.org/10.1016/j.patcog.2007.12.002

Voice, C. (2005). Online authentication: matching security levels to the risk. *Network Security, 200*5(12), 15-18. doi: http://dx.doi.org/10.1016/S1353-4858(05)70315-9

Vu, K.-P. L., Chambers, V., Creekmur, B., Cho, D., & Proctor, R. W. (2010). Influence of the Privacy Bird® user agent on user trust of different web sites. *Computers in Industry, 61*(4), 311-317. doi: http://dx.doi.org/10.1016/j.compind.2009.12.001

Vural, I., & Venter, H. S. (2012). Combating mobile spam through Botnet detection using artificial immune systems. *Journal of Universal Computer Science, 18*(6), 750-774.

Walton Cb, R. (2005). Identity infrastructure: security considerations. *Computer Fraud & Security, 2005*(8), 4-8. doi: http://dx.doi.org/10.1016/S1361-3723(05)70242-6

Weaver, A. C. (2006). Biometric authentication. *Computer, 39*(2), 96-97. doi: 10.1109/mc.2006.47

Wenjie, W., Yufei, Y., & Archer, N. (2006). A contextual framework for combating identity theft. *IEEE Security & Privacy, 4*(2), 30-38. doi: 10.1109/msp.2006.31

Whitley, E. A., & Hosein, I. R. (2008). Departmental influences on policy design. *Communications of the ACM, 51*(5), 98-100.

Wilbanks, L. (2007). The impact of personally identifiable information. *IT Professional, 9*(4), 62-64. doi: 10.1109/mitp.2007.77

William Newk-Fon Hey, T., Peter, D., & John, V. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology, 25*(2), 126-136.

Williamson, M. (2008). Technology of deception. *Engineering & Technology, 3*(17), 24-27.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58*(2), 212-222.

Xiao, Q. (2007). Biometrics-technology, application, challenge, and computational intelligence solutions. *IEEE Computational Intelligence Magazine, 2*(2), 5-9+25.

Zhenhai, D., Peng, C., Sanchez, F., Yingfei, D., Stephenson, M., & Barker, J. M. (2012). Detecting spam zombies by monitoring outgoing messages. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 198-210. doi: 10.1109/tdsc.2011.49

Joel Cherus is a PhD student at the School of Science, Engineering and Technology, Kabarak University, Kenya. He received his BSc (Computer Science) from Egerton University and a MS (Computer Science) from American Sentinel University, USA. His research interests are focused on identity management and information security.

Jason Githeko is an associate professor of Innovation and Internet Technologies at Egerton University. He received his PhD in Technology at University of Illinois at Urbana-Champaign, USA. He has previously served as Director of Egerton University Nakuru Town campus and African Virtual University Centre.His research interests are in E-learning, Computer Science Education, Web Applications, Web Engineering, Network-General, and Computer Science.

Joseph Siroris currently a part-time lecturer at Kabarak University and a Director in charge of Science, Technology, Innovation and Communication at National Economic and Social Council (NESC). He received his PhD in Engineering from Shanghai Jiao Tong University, China. His research interests are in the area of RFID and its applications in logistics and information security.

Kageni Njagi is the Director at the Institute of Postgraduate Studies and Research, Kabarak University. She received her PhD from Clemson University, USA. Her research interests are in Information Technology applications.

pISSN: 2343-6662 ISSN-L: 2343-6662 VOL. 5,No.5(2), pp 36-53, February, 2014