An Understanding Of The Cyber Security Threats And Vulnerabilities Landscape: A Case Of Banks In Kenya

Article · June 2020

CITATIONS
0

READS
191

4 authors, including:

Cpa Leonard
Jaramogi Oginga Odinga University of Science and Technology
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Solomon Ogara
Jaramogi Oginga Odinga University of Science and Technology
28 PUBLICATIONS **147** CITATIONS
SEE PROFILE

International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 7 Issue 6, June 2020

ISSN: 2394-4404

An Understanding Of The Cyber Security Threats And Vulnerabilities Landscape: A Case Of Banks In Kenya

CPA Leonard Wafula Wakoli

Dr. Solomon Ogara

Dr. Samual Liyala

Jaramogi Oginga Odinga University of Science & Technology

Abstract: ***Cyber security threats in Kenya has been increasing steadily; particularly in banks. A Cyber security vulnerability is a software, hardware or procedural weakness that may provide an attacker entry to a computer or network. This study aimed at investigating Cyber security threats and vulnerabilities that the banking industry in Kenya is grappling with. The study examined the definitions of cyber threats and vulnerabilities and further examined the categories of cyber threats and vulnerabilities afflicting organizations world-wide in general and the banking industry in Kenya in particular. We used the purposive sampling technique because the ICT functionality is centralized at the bank headquarters in Nairobi – the capital city of Kenya. The findings of the study give banks an insight on threats and hence banks must implement strategies that positively counter these threats.***

Keywords: cyber-security, cyber-crime, cyber-attack, vulnerability, applications, infrastructure

I. INTRODUCTION

A. USE OF ICTS BY BANKS

The use of information and communications technology (ICTs) by banks has greatly improved service delivery, thus making customers happier and reducing operating costs due to efficiencies that come with the technologies. Due to all the good things that come with these technologies, banks are now over-relying on the technologies. The flip side of it is that these technologies have come with a myriad of cyber threats and vulnerabilities. This echoes the assertion by Musa (2004) which indicates that cyber threats against information systems in organizations have increased as a result of increase in the use of information technology by organizations. Furthermore, the National Institute of Standards and Technology (NIST), (2014) intimate that information technology – based enterprises are highly vulnerable to a variety of cyber threats that can easily damage information systems and consequently result in financial loss. For example, hackers have been reported to be accessing bank customer accounts to steal money. According to Bhasin (2015), cyber fraud is impacting several facets of life including the financial services institutions and the banking industry very negatively.

Reasons for committing cybercrime are vast and they include monetary gain and self-satisfaction that "I can do it!" Musa (2004) posits that banks must adopt new technologies to remain competitive. For example, according to Musa (2004), customers are forcing banks to embrace new technologies such as ATMs, mobile banking, internet banking, e.t.c. The use of such technologies expose banks to cyber threats. For example, according to cyber ventures, every year, global businesses are being cost USD 500 billion by cyber-attacks – with banks being the leading targets. According to Serianu Kenya Cyber security Report 2017, the technical solutions to the complex Cyber security challenges are beyond the reach of many small and medium enterprises due to the huge resources needed. Among the top trends identified by the Serianu Africa and Kenya Cyber security Reports 2017, insider threat is one of the top threats. The two reports consider top insider threats to be (1) Administrator accounts, (2) Privileged user accounts and (3) third-parties (e.g. consultants, contractors and temporary workers).

To holistically protect banks against the cyber-attacks, we have examined the human factor exhaustively from the theoretical point of view. The role of theories such as the protection motivation theory, Institutional Theory and General deterrence Theory have been jointly examined. According to J. O. Nyawanga (2015), banks in Kenya are faced with the following: Malicious software (malware), Phishing, Pharming and Botnets or Zombies. Vulnerabilities identified by the study included the following: careless or unsuspecting employees, mobile computing, insider threats, Mobile Apps (Mpesa, Mkesho), Internet banking. The objectives of this paper are to: (1) investigate potential cyber threats and vulnerabilities that are faced by Governments, Organizations, e.t.c. globally, regionally and locally by delving into existing literature. (2) Investigate the cyber threats and understand their potential that banks operating in Kenya are grappling with.

II. LITERATURE REVIEW

A. BACKGROUND

This chapter underscores the role of banks in the economic growth of any country and explores related research work conducted previously on Cyber-threats and Vulnerabilities in financial services institutions world-over in general and Kenya in particular.

The review aims at highlighting the insights of the concepts of cyber-threats and vulnerabilities and the negative impact associated with them. The understanding of cyber threats and how they originate and their potential impact will help organizations to come up with better strategies of addressing this menace.

The role of banks world-wide in general and in Kenya in particular, is well documented as far as the economic growth is concerned. For example, the CBK 2017/2018 Annual report clearly shows that the performance of the global economy remains strong with output projected at 3.9% in 2018 and 2019 from 3.7% in 2017.

Output among the advanced economies was expected to stabilize at 2.4% in 2018 and slowdown to 2.2% in 2019. The report attributed this to the effects of escalating trade tensions among the advanced economies besides other factors. Bearing in mind the role of banks in the economic growth of any Nation, the performance of banks must be monitored with the gist of making it better all the time. For example, the CBK Board priorities in the period 2018-2021 include further modernization and strengthening of the information technology; setting up modern information and data management system through the completion of the Enterprise Data Warehouse System among other initiatives.

B. THE ROLE OF BANKS IN KENYA

The role of banks in the domestic economy is articulated through the following: (1) Financing, (2) Domestic Credit, (3) Commercial bank rates, (4) Mobile Money Transfers,(5) KEPSS Availability, (6) ACH Availability, (7) The Automated Clearing House (ACH) and (8) Cards Transactions among other areas. These functions are explained as follows:

a. FINANCING

The CBK 2017/18 Annual reports shows that the net domestic borrowing amounted to KES 273.71 billion during FY 2017/18 which was within target. In specific terms, the borrowing comprised of KES 172.82 billion from Non-Banking Financial Institutions, KES 124.27 billion from Commercial Banks, and KES 2.97 billion from Non Residents, and a repayment of KES 26.35 billion to the Central Bank of Kenya. However, Domestic financing in FY 2017/18 was 11.6% lower than in the previous year, which represents 45.0% of total financing.

From these figures, it is clear that banks play a very key role in terms of the growth of the economy of a country is concerned. Hence, should banks lose money due to cyber-attacks, the figures for financing will come down and this will impact negatively on the economy of the county where the banks are operating from.

b. BANKING SERVICES AND NATIONAL PAYMENTS

The CBK 2017/18 Annual report indicates that automation through the deployment of a payments system has resulted into a more accessible, effective and efficient Kenyan payments system – particularly with the emergence of financial technologies (Fintech).

The report shows that the dynamic nature of emerging financial technologies has opened up opportunities for innovation and growth in addition to creating challenges.

Specifically, according to the CBK 2017/18 Annual report, Mobile Money Transfer Services continued to gain popularity in the period under review For instance, the number of agents grew by 19.5% from 165,109 in June 2017 to 197,286 agents in June 2018. The number of mobile money transfer accounts increased by 24.58% from 34.18 million accounts to 42.58 million accounts during the same period. The volume and value of Mobile Phone Money Transfers increased from 1,577.68 million transactions worth KES 3,574.43 billion in FY 2016/2017 to 1,619.97 million transactions worth KES 3,747.33 billion in FY 2017/2018.

Based on this background information, it is evident that the banking industry is fully dependent on information and communication technologies (ICTs) and hence any disruption due to cyber threats and vulnerabilities will impact very negatively to the industry.

Hence, serious and spirited efforts must be made to understand cyber security threats and vulnerabilities so as to be in a vantage position to holistically tackle the problem.

C. CYBER SECURITY THREATS AND VULNERABILITY

a. CYBER SECURITY THREATS

According to Lokanadha & Bhargani (2008), a cyber-threat is “any malicious act that attempts to gain access to obtain sensitive information through online channels.” According to Antoine Bouveret (2018), successful cyber-attacks including Wannacry in May 2017 and Nopetya in June 2017 indicate that severe disruptions and loses for the targeted

organizations can be caused by cyber-attacks. Cyber threat attackers target organizations worldwide, hence, cyber threat mitigation must be looked at through the global lens. According to Robinson et al., (2013), a cyber-threat is an act that exploits cyber space with an intention of causing harm to information systems. The Kenya Cyber security Report 2017 shows that there are several cyber threats to bank electronic transactions. Such threats include insider threats which are very common particularly in the global banking sector. According to Singer & Friedman (2013), insider threat is a deliberate malicious activity by current employees who are privileged to probe systems for unauthorized access and end up taking advantage to perform illicit acts.

b. CYBER-VULNERABILITIES

According to D. L. Pip (2000); E. Bertino et al., (2010), a vulnerability is a weak point in a system or its design that enables an attack to execute an attack. In bank management information systems, vulnerabilities can occur in various areas.

For example, vulnerabilities can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems or weaknesses of the users as posited by Kizza J. M. (2013). Hardware vulnerabilities can be due to design flows and are extremely difficult to troubleshoot and fix.

Software vulnerabilities are often found in operating systems, control software such as Protocols & device drivers and Application software.

According to Abomhara M. & Koien G. M. (2015), software vulnerabilities can be caused jointly or singularly by design flaws, software complexity and human factors Human weaknesses cause technical vulnerabilities.

According to Abomhara M. & Koien G. M. (2015), technical vulnerabilities can be due to lack of user involvement, lack of sufficient resources, lacks of skills and knowledge, poor project planning, poor understanding of user requirements and incapability to manage and control the system development process. Other than these reasons, Cyber-attacks are on the rise world-wide due to the following reasons also among others: (1) Unfriendly States/Nations/Countries attack systems to gather intelligence or intellectual property. (2) Hackers seek money or make potential political statements through system disruptions. According to Kizza J. M. (2013), an attacker can be a hacker, a Cyber security criminal or a government. Examples of attacks include denial-of-service (DoS), Eavesdropping and racking. A denial-of-service attack involves rendering a computer / machine or network resource non-functional / unavailable to the indented user.

Eavesdropping means listening to a conversation taking place between two parties on real-time basis as posited by Naumann & Hogben G. (2008). Tracking means following a user's movements by the device's unique identification number (UID). This enables the offender to identify the victim so as to execute an attack. According to the Serianu Kenya Cyber security Report 2018 by Serianu, the following cyber-threats top the list of cyber-threats faced by organizations in Kenya: insider threats, cyber espionage, online mobile & Internet banking fraud, denial of service (DoS), Social media, Social engineering and VOIP PBX fraud. Denial-of-service (DoS) attacks -- Various researchers and scholars consider a "denial-of-service" attack to be characterized by an attempt by attackers to prevent /stop legitimate users of a service from using that service. Examples of denial-of-service attacks include: attempts to disrupt service to a specific system or individual and flooding a network, hence preventing authorized users from accessing the network. Carlin et al., (2015) performed several reviews on intrusion detection and prevention systems with a view of mitigating DDoS attacks in the cloud. Classification of DDoS attacks was done and the most popular DDoS attacks on the cloud systems were identified. Mahjabin et al., (2017) looked at different DDos attacks, focusing on the phases in a DDoS attack, variations and evolutions of attacks, including the attackers' targets and motivations. Zare et al., (2018) discussed intrusion detection systems and did the analysis of counter measures against DDoS attacks in terms of the location of the defense mechanisms: source-end, core-end, victim-end and distributed defense.

The Serianu Kenya 2018 Cyber security Report further shows that Cyber espionage is one of the major threats facing the country and organizations in general and banks in particular.

Hackers are on the lose stealing sensitive and valuable information such as business strategies, trade secrets, intellectual property, e.t.c. Internationally, attacks have been launched on various countries such as the United States of America (USA), China, Britain, e.t.c. The reasons for cyber espionage include to: generate revenue, gather intelligence operations, and destroy critical infrastructure of the target entities.

III. METHODOLOGY

This study used the quantitative approach to collect data for analysis and subsequent discussion.

We used both the primary and secondary data. We reviewed a variety of documents focusing on cyber security, including those from the 2014 - 2018 Africa and Kenya Cyber security Reports, the Central Bank of Kenya, and other banks like National Bank of Kenya (NBK), Technology Service Providers Association of Kenya (TESPOK), Communication Authority of Kenya (CA), Global reports from bodies like the International Telecommunication Union (ITU), among others documents from different sources. The actual data collection commenced on Friday, June 14, 2019, and it was carried out by Research Assistants (five 3rd - year students selected from Technical University of Kenya). The composition of respondents was one-ICT officer and two non-ICT professionals from each of the purposively selected banks (39). This means a total of 117 respondents were reached; constituting primary data. As for the secondary data, we used published and unpublished literature from business related journals and other related literature.

87 respondents availed the filled-up questionnaires after one-week period from 29 banks, of which 12 responses were discarded as incomplete and unusable; hence, responses from 75 respondents were used in the study for analysis.

IV. DATA ANALYSIS AND RESULTS

We performed the analysis of the collected data using SPSS 21.0 (SPSS Inc, 2007) and Microsoft Excel 2013. The results are categorized into two groups: descriptive and inferential.

A. DESCRIPTIVE STATISTICS

		Gender	Age	Edu	Duration	Dept	Postn	Terms
N	Valid	75	75	75	75	75	75	75
	Missing	0	0	0	0	0	0	0
Mean		1.27	3.61	2.97	2.80	2.45	2.60	1.51
Std. Deviation		0.445	0.853	0.464	1.027	1.427	0.493	0.665
Skewness		1.077	0.173	-0.100	-0.046	0.642	-0.417	0.965
Kurtosis		-0864	-0.711	1.878	-0.444	-0.925	-1.877	-0.197
Std. Error of Kurtosis		0.548	0.548	0.548	0.548	0.548	0.548	0.548

Table 4.1: Statistics of respondents

Table 4.1 shows that the sample had 75 respondents and there were no missing values. The standard deviations were as follows: Gender (0.445), Age (0.853), Education level (0.464), Duration (1.027), Department (1.427), Position (0.493) and Terms of engagement (0.665). Skewness values were as follows: Gender (1.077), Age (0.173), Education level (-0.100), Duration (-0.046), Department (0.642), Position (-0.417) and Terms of engagement (0.965). Kurtosis values were as follows: Gender (-0.864), Age (-0.711), Education level (1.878), Duration (-0.444), Department (-0.925), Position (-1.877) and Terms of engagement (-0.197). Standard errors for Kurtosis: Gender (0.548), Age (0.548), Education level (0.548), Duration (0.548), Department (0.548), Position (0.548) and Terms of engagement (0.548).

		Freq	%	Valid (%)	Cum. (%)
Valid	Male	55	73.3	73.3	73.3
	Female	20	26.7	26.7	100.0
	Total	75	100.0	100.0	

Table 4.2: Frequency Table for Gender

Table 4.2 shows the number of males (73.3%) and females (26.7%).

		Freq	%	Valid (%)	Cum. (%)	
Valid	20-29 years	5	6.7	6.7	6.7	
	30-39 years	32		42.7	42.7	49.3
	40-49 years	25		33.3	33.3	82.7
	50-59 years	13		17.3	73.3	100.0
	Total	75		100.0	100.0	

Table 4.3 Frequency Table for Age-range

Table 4.3 shows that most of the respondents were middle – aged; 42.7% representing the age group 30-39 and 33.3% representing the age group 40-49. Others were 17.3% representing the age of 50-59 and another 6.7% representing the age of 20-29.

		Freq	%	Valid (%)	Cum. (%)
Valid	Diploma	9	12.0	12.0	12.0
	Degree	59	78.7	78.7	90.7
	Masters	7	9.3	9.3	100.0
	Total	75	100.0	100.0	

Table 4.4: Frequency Table for Education level

Table 4.4 shows that most of the Bank employees were degree holders; 78.7%, followed by Diploma holders at 12.0% and finally and Masters Degree at 9.3%. There were no PhD holders.

		Freq	%	Valid (%)	Cum. (%)
Valid	Permanagent & Pensionable	44	58.7	58.7	58.7
	Contract	24	32.0	32.0	90.7
	Other	7	9.3	9.3	100.0
	Total	75	100.0	100.0	

Table 4.5: Frequency Table for Terms of Engagement

Table 4.5 shows that majority of the respondents were found to be on permanent and pensionable terms (58.7%) while those on contract terms were 32.0% and those on other terms like casual were only 9.3%

B. INFERENTIAL STATISTICS

a. PERCEIVED CHANGE IN THE THREATS FACING BANKS

Table 4.6 shows perceived change by respondents in terms of external attacks or fraud (e.g. phishing, website attacks).

58.7% of the respondents perceived an increase in external attacks, 6.7% perceived status quo, 22.7% perceived a decrease while 12.0% had no idea about the question that was asked.

		Freq	%	Valid (%)	Cum. (%)
Valid	Increase	44	58.7	58.7	58.7
	Same	5	6.7	6.7	65.3
	Decrease	17	22.7	22.7	88.0
	Don't know	9	12.0	12.0	100.0
	Total	75	100.0	100.0	

Table 4.6: Perceived change by respondents in terms of external attacks or fraud (e.g. phishing, website attacks)

Table 4.7 shows perceived change by respondents in terms of internal attacks or fraud (e.g. abuse of privileges, theft of information) 61.3% of the respondents perceived an increase in internal attacks, 10.7% perceived status quo, 16.0% perceived a decrease while 12.0% had no idea about the question that was asked.

		Freq	%	Valid (%)	Cum. (%)
Valid	Increase	46	61.3	61.3	61.3
	Same	8	10.7	10.7	72.0
	Decrease	12	16.0	16.0	88.0
	Don't know	9	12.0	12.0	100.0
	Total	75	100.0	100.0	

Table 4.7: Perceived change by respondents in terms of internal attacks or fraud (e.g. phishing, website attacks)

b. TARGETING (INFRASTRUCTURE VERSUS. APPLICATIONS)

Table 4.8 shows the main areas of risk in Banks for infrastructure percentagewise. 25.3% of the respondents perceived that risk through infrastructure occupied (0-19)%, 34.7% perceived that risk through infrastructure occupied (20-39)%, 16.9% perceived that risk through infrastructure occupied (40-59)%, 14.7% perceived that risk through

infrastructure occupied (60-79)%, and lastly 9.3% perceived that risk through infrastructure occupied (80-99)%.

		Freq	%	Valid (%)	Cum. (%)
Valid	(0-19)	19	25.3	25.3	25.3
	(20-30)	26	34.7	34.7	60.0
	(40-59)	12	16.0	16.0	88.0
	(60-79)	11	14.7	14.7	90.7
	>=80	7	9.3	9.3	100.0
	Total	75	100.0	100.0	

Table 4.8: Main areas of risk in Banks for infrastructure percentagewise

Table 4.9 shows the main areas of risk in Banks for Applications percentagewise. 18.7% of the respondents perceived that risk through Applications occupied (0-19)%, 5.3% perceived that risk through Applications occupied (20-39)%, 33.3% perceived that risk through Applications occupied (40-59)%,, 16.0% perceived that risk through Applications occupied (60-79)%, and lastly 26.7% perceived that risk through Applications occupied (80-99)%.

Freq	%	Valid (%)	Cum. (%)		
Valid	(0-19)	14	18.7	18.7	18.7
(20-30)	4	5.3	5.3	24.0	
(40-59)	25	33.3	33.3	57.3	
(60-79)	12	16.0	16.0	73.3	
>=80	20	26.7	26.7	100.0	
Total	75	100.0	100.0		

Table 4.9: Main areas of risk in Banks for Applications percentagewise

c. CHANGE OF THREATS IN TERMS OF INFRASTRUCTURE AND APPLICATIONS COMPARED TO PREVIOUS 12 MONTHS

Table 4.10 shows the respondents' perception of threats in terms of infrastructure. 58.7% perceived an increase of threats through infrastructure, 12.0% perceived status quo, 8.0% perceived a decrease of threats through infrastructure, and finally, 21.3% did not perceive anything.

		Freq	%	Valid (%)	Cum. (%)
Valid	Increase	44	58.7	58.7	58.7
	Same	9	12.0	12.0	70.7
	Decrease	6	8.0	8.0	78.7
	Don't know	16	21.3	21.3	100.0
	Total	75	100.0	100.0	

Source: Researcher, (2019)

Table.4.10: Respondents' perception of threats in terms of infrastructure

Table 4.11 shows the respondents' perception of threats through Applications. 48.0% perceived an increase of threats through Applications, 25.3% perceived status quo, 9.3% perceived a decrease of threats through Applications, and finally, 17.3% did not perceive anything.

		Freq	%	Valid (%)	Cum. (%)
Valid	Increase	36	48.0	48.0	48.0
	Same	19	25.3	25.3	73.3
	Decrease	7	9.3	9.3	82.7
	Don't know	13	17.3	17.3	100.0
	Total	75	100.0	100.0	

Table.4.11: Respondents' perception of threats through Applications

d. KIND OF ATTACKERS THAT ARE THE THREE MOST LIKELY TO TARGET BANKS IN THE NEXT 12 MONTHS FROM THE TIME OF STUDY

Table 4.12 shows the respondents' perception about external attackers in Banks. 5.3% perceived external attackers to be anonymous, another 5.3%perceived external attackers to be criminal groups, 25.3% perceived external attackers to be hobbyist hackers, 58.7% perceived external attackers to be insiders and finally, 5.3% thought external attackers were competitors.

		Freq	%	Valid (%)	Cum. (%)
Valid	Anonymous	4	5.5	5.3	5.3
	Criminal groups	4	5.3	5.3	10.7
	Hobbyist hackers	19	25.3	25.3	36.0
	Insiders	44	58.7	58.7	94.7
	Competitors	4	5.3	5.3	100.0
	Total		75	100.0	100.0

Table.4.12: Respondents' perception of external attackers

e. COMMON TYPES OF CYBER THREATS TO BANKS

Table 4.13 shows the respondents' take on the common threats to Banks. 8.0% perceived Account take-over as one of the common types of cyber threats to Banks. 33.3% considered Identity theft as a common threat and finally, 58.7% viewed insider threats as a big problem

		Freq	%	Valid (%)	Cum. (%)
Valid	Account take-over	6	8.0	8.0	8.0
	Identity theft	25	33.3	33.3	41.3
	Insider threats	44	58.7	57.8	100.0
	Total		75	100.0	100.0

Table.4.13: Respondents' take on common Cyber threats to Banks

V. DISCUSSION, CONCLUSION AND FUTURE STUDIES

A. DISCUSSION OF RESULTS

The exponential use of ICTs by banks and bank customers has increased security and privacy risks. Most of such risks could be attributed to device vulnerabilities that arise from cybercrime by fraudsters and misuse of system resources. For example, a bank in Kenya lost millions of shillings through the compromising of ATMs in December 2018. Related cases have been reported elsewhere. Banking transaction devices should be designed in such a way that safe and ease of usage are guaranteed.

The need to understand threats and vulnerabilities should not be gainsaid. This is so as to put in place sufficient mitigation mechanisms. More so, understanding potential attacks enables system developers to take security features of the systems very seriously and know the resources required to enhance security of the systems they develop. To mitigate

both potential threats and their consequences, there is need for further research to fill the gaps in knowledge concerning threats, vulnerabilities and cybercrime. Also necessary steps should be provided to mitigate probable attacks.

B. CONCLUSION

Banks have embraced the use of internet technologies to the extent that they cannot afford downtimes; including non-working hours. This is because most of the banks have customers who are technology savvy, hence hardly go to banking Halls for bank services but instead access their bank accounts through their mobile phones on a 24/7 basis. Bank ICTs face various cyber threats and have a lot of vulnerabilities that need to be identified for effective protective action to be taken. In this paper, Cyber security threats and vulnerabilities facing financial institutions and banks were introduced.

The main aim of the study was to investigate Cyber security threats and vulnerabilities encountered by banks in Kenya. Cyber security goals are comprehensively outlined and the discussion focuses on the need to understand threat vectors so as to counter them effectively.

Further research areas are suggested such that if they are researched on, the mitigation would be more elaborate. It is hoped that this study will be useful to future research work in the Cyber security arena as the zeal to identify and understand cyber threats and vulnerabilities continue to attract a lot of interest.

REFERENCES

[1] A. Carlin; Hammoudeh, M.; Aldabbas, O 92015). Defence for Distributed Denial of Service Attacks in Cloud Computing. Procedia Comput. Sci., 73, 490–497.
[2] A. Musa (2004). Responses by Commercial Banks operating in Kenya to Threats and changes in the environment. A case study of National Bank of Kenya, Unpublished MBA Project.
[3] Antoine Bouveret (2018). Cyber risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper wp/18/143.
[4] E. L. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini (2910). "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, pp. 25–44.
[5] I. Naumann & G. Hogben.(2008) "Privacy features of european eid card specifications," Network Security, vol. 2008, no. 8, pp. 9–13.
[6] J. M. Kizza J. M., (2013). Guide to Computer Network Security. Springer.
[7] J. O. Nyawanga.(2015). Meeting the challenge of cyber threats in emerging electronic transaction technologies in Kenya Banking Sector.
[8] Lokanadha M. & Bhargavi. (2018). America International Journal of Research in Humanities, Arts and Social Sciences, 21(1), Pp 65-71
[9] M. Abomhara & G. M. Koien (2015) Cyber-security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber-security, Vol. 4, 65–88. doi: 10.13052/jcsm2245-1439.414
[10] M. Bhasin Lal (2015) An Empirical Study of Frauds in the Banks. European Journal of Business and Social Sciences, Vol. 4, No. 07,. Available at SSRN: https://ssrn.com/abstract=2703640
[11] National Institute of Technology and Standards (NIST) (2014). "Framework for Improving Critic Infrastructure Cyber security version 1.0"(Cyber security Framework), http://www.nist.gov/cyberframework/upload/Cyber security-framework-021214-final.pdf
[12] P. W. Singer, & A. Friedman (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.
[13] T. Mahjabin; Y. Xiao; G. Sun.; W. Jiang (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw., 13.
[14] Zare, H.; Azadi, M.; Olsen, P. (2018). Techniques for Detecting and Preventing Denial of Service Attacks (a Systematic Review Approach). In Advances in Intelligent Systems and Computing—In Information Technology-New Generations; Springer: Cham, Switzerland; Volume 558, pp. 151–157.