(IJRST) 2018, Vol. No. 8, Issue No. II, Apr-Jun **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

AUTHENTICATION AND SECURITY MEASURES IN INTERNET BANKING: EMPLOYABILITY OF ALTERNATE APPROACHES ENHANCE THE DETECTION AND ADOPT COUNTERMEASURES TO CURB DATA BREACHES

GATIK GOLA
Student, King's College, Taunton, UK

ABSTRACT

Cloud computing is a popular theme of research in information systems. It has revolutionized the perspective of distributed computing from existing methods. This process is prone to security threats to the information and data which is currently moved from on-premises to off-premises, even though cloud computing is beneficial. Due to the openness of data, cloud computing has been experiencing security threats that must be overcome for this service to be fully utilized. One such threat is data breach, this is because data is stored in different places across the globe hence difficult for security to be monitored. Therefore, security and privacy of data are the two major concerns of users in the cloud technology. Internet banking applications have become popular within banks and almost each bank has got its own service. The login and signature security depend on the user/static password authentication method to certificates and tokens. Considering the confidentiality of this information, for instance passwords and bank accounts, banks need to identify, evaluate and solve distinct risks to security in regard to cloud computing in their management information security system. This paper sought to establish the available security measures employed in curbing data breaches, their shortcomings and suggest possible solutions. The paper employed a descriptive survey research design; a pre-tested questionnaire was used to collect data from the 46 banks that use internet banking in Kenya. The study found that the banks had employees who were certified in security matters but none was certified in cloud computing security and recommended Staff Training and certification on Cloud Computing Security, cloud computing and resource management.

Since its inception Internet has got the solutions to all the technological problems. However, over the past few years, cloud computing model has seen a large shift towards its adoption, and it has become a trend in information technology with its advantages [1]. The advantages of using cloud computing include decreased hardware maintenance cost, increased user-friendliness and flexibility of highly automated processes.

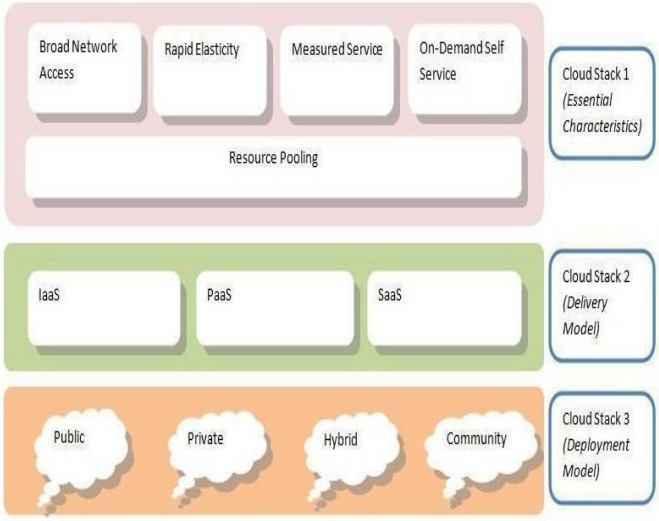

Fig 1: Architecture of Cloud computing [2] (Dahal, 2012)

Data breach is an incident in which sensitive, protected or private data has possibly been viewed, pilfered or used by an individual who doesn't have the authority to do so [3].

Keywords : *Curbing; Cloud computing; Cloud security; internet banking; data breaches*

INTRODUCTION

In a time of data and globalization, a ton of computing power is required to spread business experiences and have an upper hand. Associations information is prepared by utilization of the processing power created by their in-house server networks. Notwithstanding, working a private server company to measure up with quickly developing information handling solicitations can be complicated and costly. Distributed computing gives an option. Being a term known for web-based processing, cloud computing was propelled by industry monsters including Google Inc., Amazon.com in late 2006. It guarantees to furnish on request processing power with quick execution, low support, and less IT staff at affordable prices.

Most common causes of data breaches within organizations can be as follows; physical loss or theft of devices, Weak Security Controls Operating system and application vulnerabilities, Internal Threats, and Malicious Attacks [4]

Cloud computing simply means the interconnected and virtualized arrangements and resources that are dynamically provisioned and presented as a platform for users to run their application from anywhere in the world[5]. Banking system continues to be sensitive as expected to the progress and development needs of all the segments of the society. But until lately it has not been having a great time dealing with the acute aspects of cloud computing. In an in-depth research by Islam and Beg in 2016 had the research forecasted that by the end of the year 2016 poor return from equity will drive 60% of all the banks around the globe to start processing most of their transactions in the cloud [6].

A survey carried out by IDC enterprise showed that 74.6% of the candidates identified security as a threat to adopting cloud.

In the year 2011 Barclays bank UK one of the big financial institutions in the world adopted cloud computing in partnership with IBM [7] Kenneth Merritt, the then head of infrastructure and service delivery is one man who went ahead to explore the banking services that Barclays could use in the cloud, Merritt had been working with IBM to promote the retail banking business's infrastructure by embracing the idea of pay as you go model with internal customer.

In November 2015, an examination was done to find out how Tesco Bank in the UK had adopted cloud computing services for the past eight months [8], Tesco bank had moved from zero cloud facility to making the company proficient at business in a little over that eight-month period. The journey to adoption of cloud started out with a single webpage for insurance comparison site Tesco compare which was hosted for a closed part of its business. It then developed in a haste to cover other applications, like mobile applications for the then new Tesco Drive car insurance that measures how a person drives and adjusts its insurance premiums. Just from a simple start, the bank went from a single 'out-of-service' web page to building 'compliant AWS VPCs'(virtual private clouds) as an extension to their data center, applied production workloads and launched our AWS Tesco drive application.

A username is a useful way to directlypresent yourself to a computer, program or application. This is then backed up by the password which confirms that you are the person who you are saying you are. The security of username is often overlooked when one is thinking about being secure while online which is said to be a wrong perception while more significance is given to password. If your password doesn't link correctly with the username, then the application or the service will not open up as per your demand. There are different methods in the way passwords are stored in the cloud, some are more secure than others but they still pose a challenge [9]. It has been recorded that the use of usernames and passwords is the most sharedverification method used to control access to information although they are also recognized as being extremely weak protection [10]. There are different ways through which password-protected systems can be attacked easily by an intruder, this can be through password guessing, Dictionary attacks, Login spoofing and eaves dropping.

Fig 2: Example of an authentication page using username and password

OTP is a password that is only valid for one login session ortransaction, be it on a computer system or even digital device. OTPs are designed to have two main variables, this are the passphrase length and the number of times the one-time password should be hashed [11]. You tend to be on a higher security level if your passphrase is long, as it is difficult to decipher to long a password. It should be noted that the longer a passphrase, the harder it will be for the user to remember. Therefore, care is required for optimal web protection and proper functioning of the OTP system.

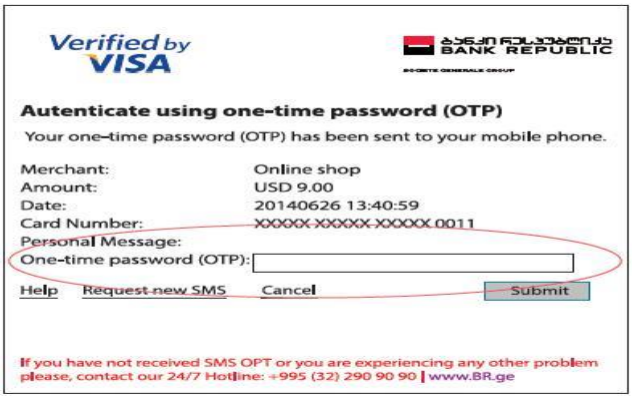

Fig 3: An example of OTP log in page from 3D secure service

As more and more businesses are doing transaction throughthe Internet, a great responsibility of protecting the data comes along with it[12]. Identity authentication technology is pivotal to protect the private things stored on the databases[13]. One Time Password also faces numerous challenges like Replay attacks, Impersonation attacks and pre-play attacks

Biometrics is the automatic identification of a person based on some physical or behavioralattributes which can be fingerprint, face shape or voice [16].Biometrics is not used everywhere instead passwords are, nothing can be perfect and biometrics as an authentication method has its own shortcomings [17].Systems using biometrics still has a need especially to be improved in the terms of speed and accuracy. Biometric systems have a false rejection rate under 1%, and reasonably low false acceptance rate are still very in the existing biometrics technology. Even though few biometric systems are quick and precise when it comes to low false acceptance rate enough to allow identification and also automatically recognizes the user identity. Current systems are mostly applicable to verification only, as the false acknowledgement rate is too high [18].

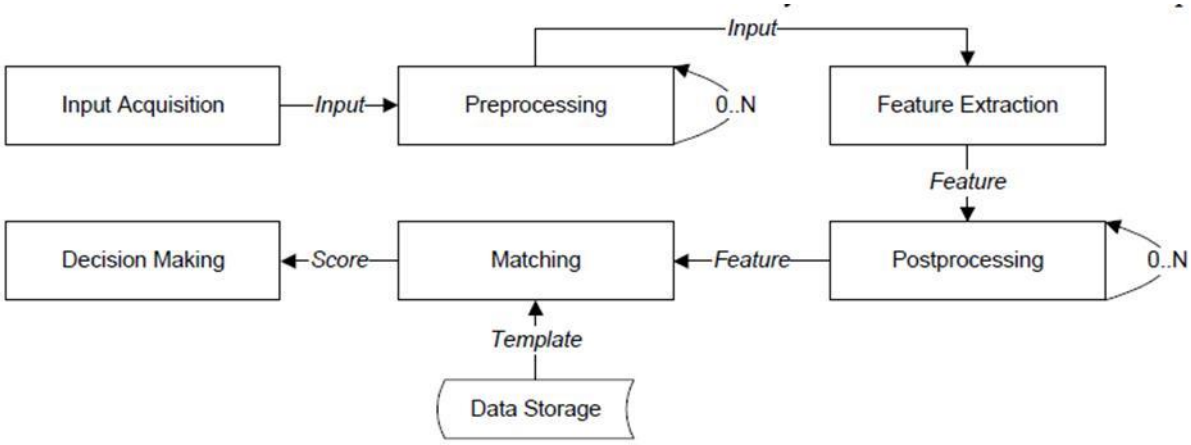

Fig 4: General Flow of Biometric System

The rest of the paper is organized as follows, we first highlight on related works on curbing data breaches in section 2, Section 3 focuses on methodology, then the next section which is section 4 discuss the results and section 5 discusses the proposed measures while section 7 describes the conclusion together with the future works.

Cryptzone [21] offers products which are commercially available while dealing with data security. This includes products in a wider range that can be encrypted, and these products offerprotection to the sensitive data.

Schmidt et. al. [22], have presented the TrustBox, a security architecture for preventing data breaches. The approach proposed provides a platform, network and security when offline. Categorization of data is said to be sensitive and insensitive and then corresponding applications are isolated by use of virtualization technology. Through introduction of a multi-lane network architecture and encrypting of virtual hard disk, data theft or loss accidentally is prevented, whenever

offline, an offline mode will then handle data transfer and encryption. Biometric feature vector together with a smartcardsetup handles the authentication. Implementation of TrustBox is based on virtual Box and Java card.Kumar et. al. [23], have proposed a technique called elliptic curve cryptography. The model consists of two parts in the cloud storage server, namely the private data and the shared data section. The two sections of the cloud data storage make data sharing accessible and secure. The user private data will be stored in the private data section; whereas, data that needs to be shared amongst the selective users will be stored on the shared data section. Their approach further highlights that data stored in the cloud and flow as plain text through the network is a security threat, the data accumulated in both sections (private and shared data section) will be encoded using the elliptic curve cryptography approach.

The study was performed in 15 major banks in Kenya that have adopted internet banking based on cloud.

A descriptive survey was conducted in fifteen major banks in Kenya that have adopted internet banking. A pre-tested questionnaire was sent via email to forty six (46) respondents in the 15 different banks in the sampling frame. In each bank, IT experts were purposively selected depending with their availability.

Primary data, both qualitative and quantitative was collected from the IT experts. Secondary, qualitative data (literature review) was obtained from books, journal papers, previous theses, conference proceedings, magazines and the internet.

Data was collected on respondent organization cloud model usage, the cloud model available were IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a service)

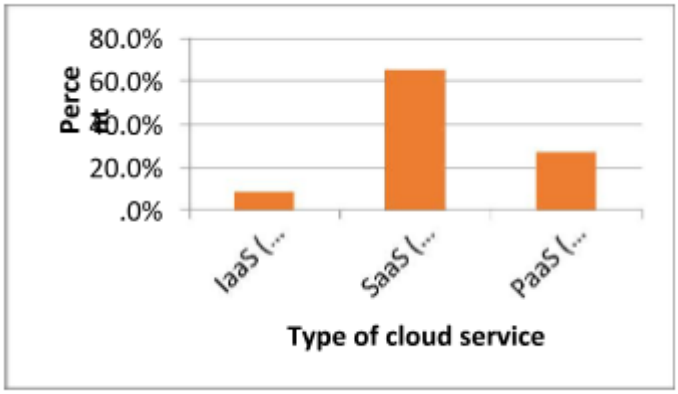

Fig 5: Cloud service models used in respondents organization

The findings on the type of cloud used by the banks indicated that Infrastructure as a service usage was 8.3% this was the lowest recorded, 65% usage was recorded by software as a service which was the highest cloud service used, platform as a service model usage was 26.7%.

The research tried to establish the departments where the respondents were drawn from.

Table 1. Job designation of Respondents

	r requency	***Percentage***	*Percentage*	*ercentage*
Credit Officer	1	2.2	2.2	2.2
Customer Service officer	1	2.2	2.2	4.3
Digilife Team Leader	3	6.5	6.5	10.9
Enterprise Application Engineer	2	4.3	4.3	15.2
IT Associate	2	4.3	4.3	19.6
IT Manager	3	6.5	6.5	26.1
IT Support	28	60.9	60.9	87.0
Product Manager	2	4.3	4.3	91.3
Project Asst. Manager	1	2.2	2.2	93.5
Project Lead ICT	2	4.3	4.3	97.8
Project Manager	1	2.2	2.2	100.0
Total	46	100.0	100.0	

Table 2. reveals that out of the IT staff members in the possible banks studied, IT Support staff members were the majority (60.9%) indicating that issues to do with security measures for curbing data breaches in the internet banking is majorly handled by the IT support staff. The other staffs 39.1% are also knowledgeable in security issues as a general and are able to support and advise the I.T staff.

The study investigated the duration the respondents had interacted with cloud computing. The results indicate that Sidian bank had the highest mean of 4 an indication that majority of the respondents had interacted more with the cloud, Barclays bank of Kenya came second with a mean of 3.7. Eco Bank, CFC Stanbic, I&M and KCB were had a least mean of 2.0, this showed that the respondents from this organization had interacted less with Cloud. The analyzed data is shown in the figure below

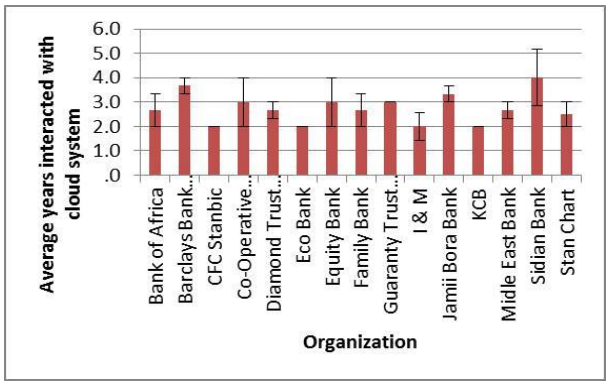

Fig 6: Duration of the Respondent Interaction with the cloud

Security Measures used

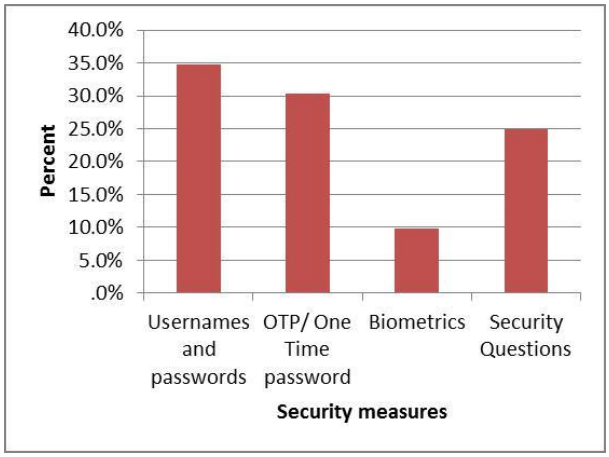

Fig 7: Security measures used by respondents' organisation

The findings established that banks could use more than one security measure to enhance security; there was combination of two, three and even up to four security measure at ago. The usage of usernames and passwords among all the banks was at 34.8%, this was the highest in percentage in

terms of security measure being used, and this is totally opposite to what others have proposed. [19] asserts that the lack of standard rules to guide a user in choosing of username and password has made it a challenge for users to remember the login credentials. OTP/One Time Password also recorded highest usage after username and password of 30.3% this implied that most of the banks were using it at that time of study. Biometrics recorded a 9.8% usage which was the lowest security measure usage. Security Questions usage recorded a usage of 25%.

Efficiency of Security Measures

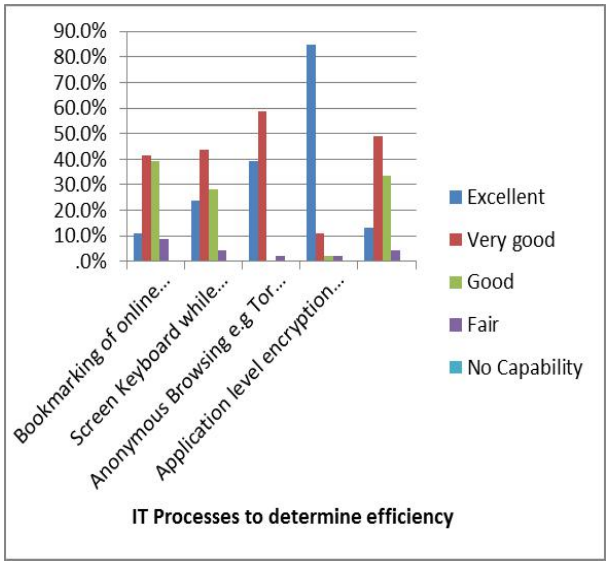

Fig 8: Efficiency of security measures

Data breaches increase has led to banking institutions want to secure their data especially within the cloud. The study revealed that most of the respondents from the banking

Results on the perceived effectiveness of different security measures showed that 10.9% of the respondents rated use of bookmaking of online web address as excellent, 41.3% thought it was very good, 39.1% of the respondents said it was good, 8.7% of the respondents thought it was fair and zero percentage did not settle for no capability.

Findings also revealed that 23.9% of the respondents felt that the use of onscreen keyboard while accessing internet banking websites was excellent, 43.5% rated it as very good, 28.3% of the respondents thought it was good a further 4.3% thought it was fair a zero-percentage rated it as of no capability.

On usage of anonymous browsing an example being tor for protection of personal data 39.1% of the respondents rated it as excellent, 58.7% of the rated anonymous browsing as very good, zero percentage thought it was good, 4.3% rated it as fair and further zero percentage thought it had no capability.

Application level encryption was another security measure that was looked into, 84.8% of the respondents thought that it was excellent, 10.9% of the respondents it as very good, 2.2% rated it as good and zero percentage rated it as on no capability.

Finally, on the use of established web browsers, 13.5% of the respondents rated it as excellent, 48.9% rated it as very good, 33.3% of the respondents thought it was good, 4.4% rated it as fair and zero percent rated it as with no capability.

The approaches proposed in this paper as security measures were in line with what the respondents desired. This are easily available measures which are already in existence and not complicated in nature even though they have not been utilized by this organizations and would help in curbing data breaches if adhered to, therefore the proposed approaches can be easily executed within a short period of time, and they will not be costly to the organizations. The following approaches were proposed as the security measures.

Bookmarking is saving a shortcut that directs a browser to a specific webpage, the URL, favicon and link are stored. Saved bookmarks of online banking address will allow you visit the right URL, since users are not keen to URLs and thus avoid visiting misleading online banking addresses that have been created by attackers.

Major threat to online banking transactions has been spyware, one of the most serious privacy risks that arises when a spyware is installed in a computer is password hijacking or keylogging. Key logger will capture all keystrokes used by a user, this includes login credentials like username and password, on screen keyboard is a visual representation of the standard keyboard that can be installed and used on screen. Use of on screen keyboard is a method to winning key loggers [20]. Internet banking website log in page needs to have their own on screen keyboard.

Anonymous browsing is surfing the internet while hiding the personal identifiable information when using the World Wide Web, this has aid in users protecting their personal data and meet the daily increasing demand for web privacy protection

For internet banking users to feel secure then banks need to follow suit by advising their clients to use anonymity while doing their transactions.

In application level encryption data is encrypted in the application that has been used to come up with data or has been used to modify that data, instead of data being encrypted after it reaches the database it is encrypted before it written to the database. This ensures that sensitive information about internet bank users is well protected and encryption to each user data is unique.

A browser as it is commonly known is an application software that is used to search, retrieve and present information in the World Wide Web. Browsers with weak security features can be easily targeted. Many organizations usually tell their clients which web browsers to use because of the enhanced security features. Use of established web browser ensures security to the user’s data.

In conclusion, there are enormous security challenges in internet banking based on cloud. This paper has tried to address common challenges and the proposed security measures that can be adopted to ensure safeguard of data. The security measures are cost friendly and easier for adoption, to ensure the benefits of cloud computing the following are the recommendations.

i. The banks should train their clients in usage of some of the proposed security approaches, use of established web browsers and bookmarking of the internet banking websites should be encouraged.

ii. Continuous training of staff on emerging challenges on cloud computing and how to curb these challenges.

iii. Clear guidelines on security measures and governance should be designed.

At this end, it worth to not that there are few other areas that can be looked into as future work, there is need to asses other challenges that might be of risk to internet banking, this paper only touched on data breach but there are still other security concerns, secondly the issue of policy and guidelines of data in cloud computing. There should be clear policy on cloud computing.

REFERENCES

[1] Bhadauria, R., &Sanyal, S. (2012). Survey on Security Issues in Cloud Computing Associated Mitigation Techniques. International Journal of Computer Applications, IJCA, 47-66

[2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[3] Dahal, Sanyal. (2012). Security Architecture for Cloud Computing Platform.

[4] TechTarget's IT Encyclopaedia. (n.d). *What is DataBreach?-Definition from Whatls.com*. Retrieved fromhttp://searchsecurity.techtarget.com/definition/data-breach

[5] Orion Blog. (2015). *Most Common Causes of DataBreaches. Retrieved March 17, 2016 from*. Retrievedfrom http://www.oriontech.com/most-common-causes-of-data-breaches/

[6] Suresh, S., Huang, H., & Kim, H. J. (2015). Scheduling in compute cloud with multiple data banks using divisible load paradigm. *Aerospace and ElectronicSystems, IEEE Transactions on*, 1288-1296.

[7] Islam, M., Islam, K., & Beg, N. (2015). Paradigm shift towards cloud computing for Banking sector. *2015International Conference on Computer and Information Engineering (ICCIE)*, (pp. 126-129). Rajshahi: IEEE.

[8] Goldsmith, J. (2011, 05 23). *Barclays partners with IBMfor private cloud project*. Retrieved from CIO:http://www.cio.co.uk/insight/it-strategy/barclays-partners-with-ibm-for-private-cloud-project-3431613/

[9] Finnegan, m. (2015, November 17). *Computer WorldUK*. Retrieved from How Tesco Bank moved to AWS cloud in eight months: http://www.computerworlduk.com/cloud-computing/how-tesco-bank-has-adopted-aws-cloud-as-business-as-usual-in-eight-months-3629767/

[10] Gordon, W. (2012, June 20). how your passwords are stored on the internet and when your password stregthdoesnt matter.

[11] Kessler, G. C. (2007). Passwords — Stregths and Weaknesses. *Internet and Internetworking Security*.

[11] Ben Soh, A. J. (2003). A novel Web security evaluation model for a one-time-password system. *Web Intelligence,2003. WI 2003. Proceedings. IEEE/WIC International Conference on*, (pp. 413-416). Halifax, NS, Canada.

[12] Huiyi, L., &Yuegong, Z. (2013). An improved one-time password authentication scheme. *CommunicationTechnology (ICCT), 2013 15th IEEE International Conference on* (pp. 1-5). Guilin: IEEE.

[13] Lamport, L. (1981). Password Authentication with Insecure Communication", In: Comm. ACM, .*Communication and Security*, 770-772.

[14] Shang, T., &Gui, L. Y. (2015). Identification and prevention of impersonation attack based on a new flag byte. *2015 4th International Conference on ComputerScience and Network Technology (ICCSNT)* (pp. 972-976). Harbin, China: IEEE.

[15] Bond, M. (2012, 09 10). *Chip and Skim: cloning EMVcards with the pre-play attack.* Retrieved from Light Blue Touch Paper: https://www.lightbluetouchpaper.org/2012/09/10/chip-and-skim-cloning-emv-cards-with-the-pre-play-attack/

[16] Kautsar, S., Akbar, S., &Azizah, F. N. (2014). An application framework for evaluating methods in biometrics systems. *Data and Software Engineering(ICODSE), 2014 International Conference* (pp. 1-6).Bandung: IEEE.

[17] Maty´aˇs, V., & ˇR´ıha, Z. (n.d). Biometric Authetication, Security and Userbility.

[18] Defence, D. o. (2005). Trusted Computer System Evaluation Criteria.

[19] Nasirinejad, M., &Alireza, A. Y. (2012). SASy Username and Password Management. Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, 242-246.

[20] Raymond. (2014). *5 Virtual Keyboards Tested toDetermine their Effectiveness Against Keyloggers.* Retrieved from Raymond cc. Computers Made Easy: https://www.raymond.cc/blog/how-to-beat-keyloggers-to-protect-your-identity/

[21] Cryptzone. Cryptzone. http://www.cryptzone.com, February 2018.

[22] Schmidt, M., Fahl, S., Schwarzkopf, R., &Freisleben, B. (2011). TrustBox : A Security Architecture for Preventing Data Breaches. https://doi.org/10.1109/PDP.2011.44

[23] Kumar, A., Lee, B.G., & Lee, H.(2012). Secure Storage and Access of Data in Cloud Computing, 336-339.