

# Approaches to Curbing Data Breaches in Internet Banking based on Cloud computing

Okiyai Otieng

School of Computing &  
Information Technology  
Jomo Kenyatta University of  
Agriculture & Technology

George Okeyo

School of Computing &  
Information Technology  
Jomo Kenyatta University of  
Agriculture & Technology

Wilson Cheruiyot

School of Computing &  
Information Technology  
Jomo Kenyatta University of  
Agriculture & Technology

## ABSTRACT

Cloud computing is a popular theme of research in information systems. It has revolutionized the perspective of distributed computing from existing methods. Although cloud offers great benefits, it does introduce security threats to the information and data which is currently moved from on-premises to off-premises. Due to the openness of data, cloud computing has been experiencing security threats that must be overcome for this service to be fully utilised. 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 vary from user/static password authentication method (it is alleged as the weakest way to manage one's accounts) 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

## Keywords

Curbing, Cloud computing, Cloud security, internet banking, data breaches

## 1. INTRODUCTION

In an era of information and globalisation, a lot of computing power is required to propagate business insights and competitive advantage. Organizations data is processed by use of the computing power generated by their in-house data centres. However, operating a private data centre to measure up with rapidly growing data processing requests can become complicated and costly. Cloud computing gives an alternative. Being a term known for internet-based computing, cloud computing was launched by industry giants including Google Inc., Amazon.com in the late 2006. It promises to provide on demand computing power with quick implementation, low maintenance, and fewer IT staff at lower costs.

Since its inception Internet has become a driving force towards the different technologies that have been developed. However, over the past few years, cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in information technology with its promises [1]. The advantages of using cloud computing include reduced hardware maintenance cost, easy accessibility across the globe and flexibility of highly automated processes.

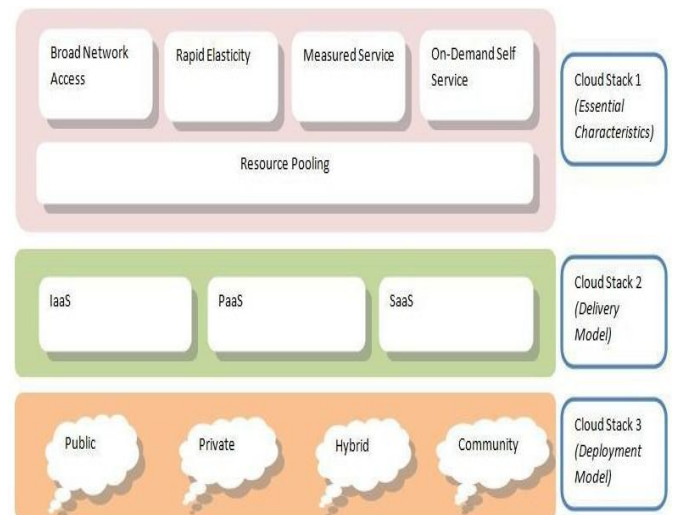


Fig 1: Architecture of Cloud computing [2] (Dahal, 2012)

Data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual who is not authorized to do so [3].

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]

## 1.1 Cloud Computing and Internet Banking

Cloud computing simply means the interconnected and virtualized infrastructures and resources that are dynamically provisioned and presented as an artificial platform for end users to run their applications 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 the banking sector has not been able to embrace the extensive functionalities of the 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 the banks worldwide to start processing majority of their transactions in the cloud [6] even though a survey carried out by IDC enterprise panel 74.6% of the participants identified security as the threat to adopting cloud.

### 1.1.1 Barclays Bank Cloud it.

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 upgrade the retail banking business's infrastructure by adopting a pay as you go model with internal customer.

### 1.1.2 Tesco Bank adopts Cloud

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 hardly using the cloud to making it as business as usual 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 monitors how a person drives and adjusts its insurance premiums. Just from a simple start, the bank went from a single 'out-of-serice' web page to building 'compliant AWS VPCs'(virtual private clouds) as an extension to their data centre, implemented production workloads and launched our AWS Tesco drive application.

## 1.2 Authentication and Security Measures in Internet Banking

### 1.2.1 Usernames and passwords

A username is a way to instantly introduce yourself to a computer, program or service, 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 importance is given to password. Your password must have a valid username linked to it, otherwise it won't allow access to your computer, application or service. 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 common form of authentication used to control access to information although they are also recognised as being extremely poor form of 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.

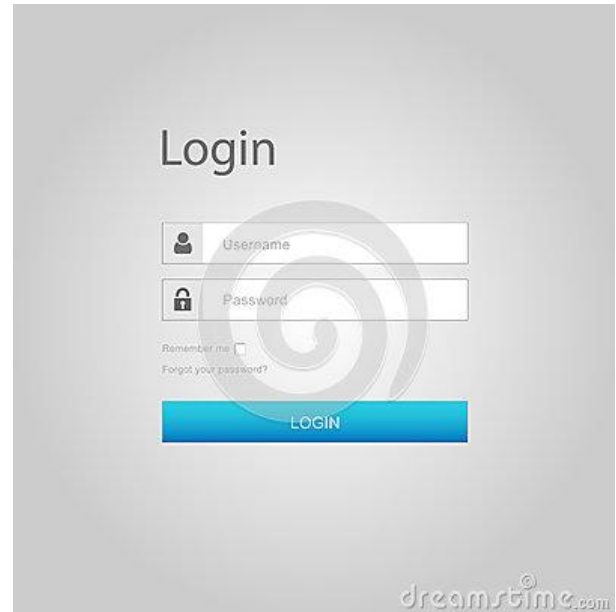


Fig 2: Example of an authentication page using username and password

### 1.2.2 One Time Password (OTP)

OTP is a password that is only valid for one login session or transaction, be it on a computer system or even digital device. OTPs are designed to have two main variables, these are the passphrase length and the number of times the one-time password should be hashed [11]. It's a known fact that the larger the passphrase length the better the security it offers. 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 security and usability of the OTP system.

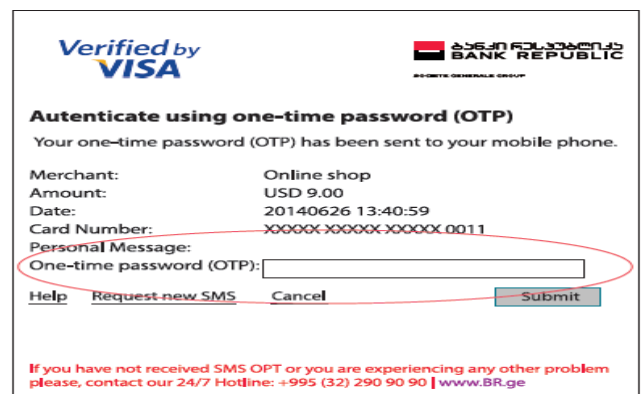
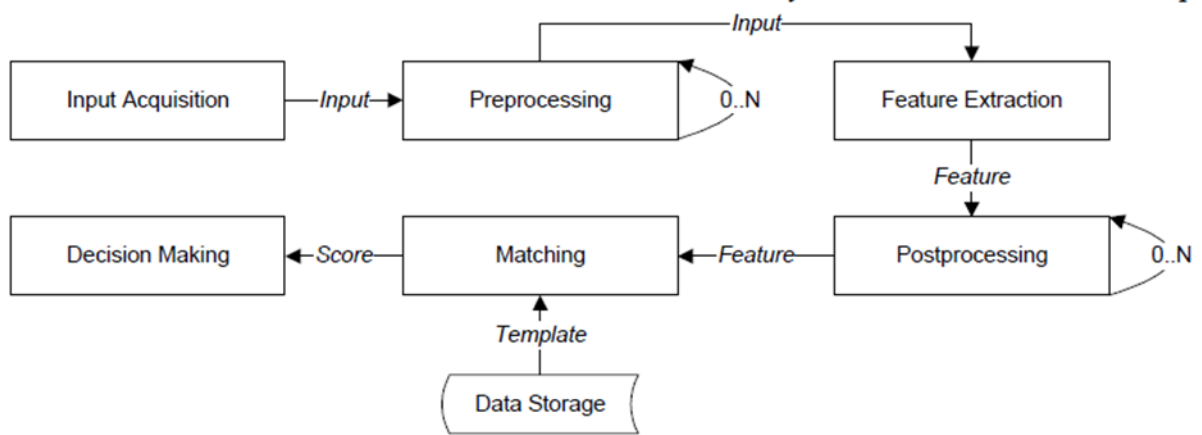


Fig 3: An example of OTP log in page from 3D secure service

As more and more businesses are doing transaction through the Internet, great attention should be paid to the security of information [12]. Identity authentication technology is the first protector and the portal of network system [13]. One Time Password also faces numerous challenges like Replay attacks, Impersonation attacks and pre-play attacks

### 1.2.3 Biometrics

Biometrics is the automatic identification of a person based on some physical or behavioural characteristics which can be fingerprint, face shape or voice [16].Biometrics is not used everywhere instead passwords are, nothing can be perfect and



**Fig 4: General Flow of Biometric System**

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 fast and accurate when it comes to low false acceptance rate enough to allow identification and also automatically recognizes the user identity, current systems are mostly suitable for verification only, as the false acceptance rate is too high [18].

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.

## 2. RELATED 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, products such as USB stick, file encryption and hard disk, this products offers sensitive data being kept way from unauthorized persons.

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 smartcard setup 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 consist 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 makes data sharing easy and secure. The user private data will be stored in the private data section whereas data that needs to be shared amongst the trusted 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 stored in both sections (private and shared data section) will be encrypted using the elliptic curve cryptography approach.

## 3. METHODOLOGY

### 3.1 Area of Study

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

### 3.2 Population

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.

### 3.3 Data Collection

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.

## 4. RESULTS AND DISCUSSIONS

### 4.1 Cloud Service Model used

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)

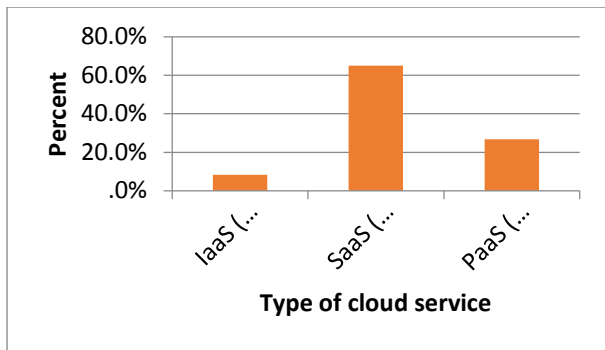


Fig 5: Cloud service models used in respondents organization

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%.

#### 4.2 Job Designation of the Respondents

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

Table 1. Job designation of Respondents

	Frequency	Percentage	Validity Percentage	Cumulative percentage
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.

#### 4.3 Duration of Interaction with Cloud

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 analysed data is shown in the figure below

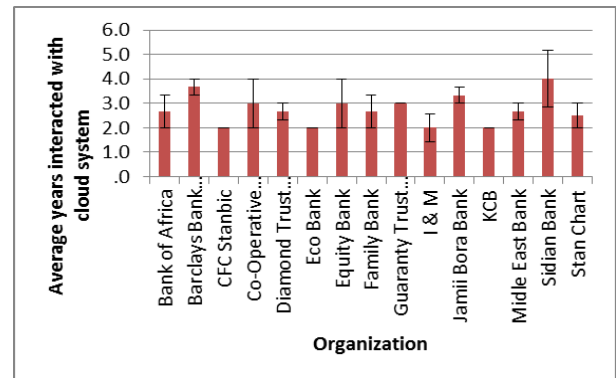


Fig 6: Duration of the Respondent Interaction with the cloud

#### 4.4 Security Measures used

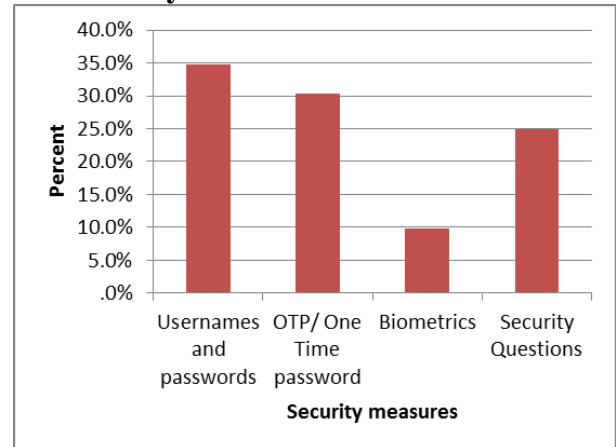


Fig 7: Security measures used by respondents' organisation

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%.



## 4.5 Efficiency of Security Measures

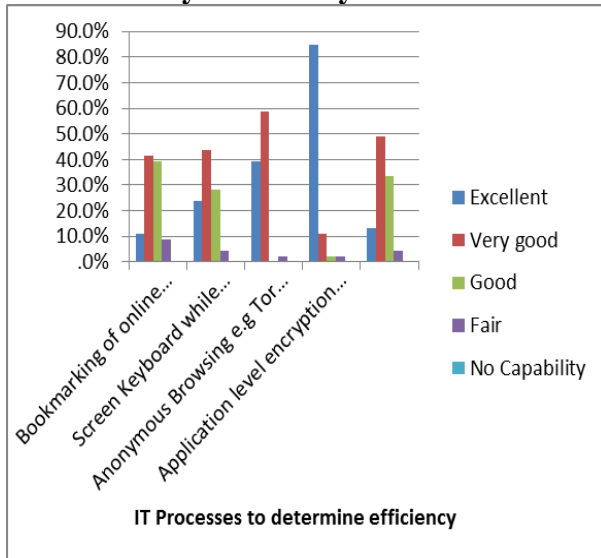


Fig 8: Efficiency of security measures

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 bookmarking 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.

## 5. PROPOSED SECURITY MEASURES

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 utilised by this organizations and would help in curbing data breaches if adhered to, therefore the proposed approaches can be easily implemented within a short period of time and will not be costly to the organizations. The following approaches were proposed as the security measures. The res

## 5.1 Bookmarking

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.

## 5.2 Use of on screen keyboard

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 keyloggers [20]. Internet banking website log in page needs to have their own on screen keyboard.

## 5.3 Anonymous Browsing e.g Tor

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.

## 5.4 Application level encryption

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.

## 5.5 Use of established web browsers

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.

## 7. CONCLUSION AND FUTURE WORK

There are enormous security challenges in internet banking based on cloud, this paper has tried addressing common challenges, the proposed security measures 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 this 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.

## 8. REFERENCES

- [1] Bhadauria, R., & Sanyal, S. (2012). Survey on Security Issues in Cloud Computing Associated Mitigation Techniques. *International Journal of Computer Applications, IJCA*, 47-66Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.
- [2] Dahal, Sanyal. (2012). Security Architecture for Cloud Computing Platform.
- [3] TechTarget's IT Encyclopaedia. (n.d). *What is Data Breach?-Definition from Whatls.com*. Retrieved from <http://searchsecurity.techtarget.com/definition/data-breach>
- [4] Orion Blog. (2015). *Most Common Causes of Data Breaches*. Retrieved March 17, 2016 from. Retrieved from <http://www.oriontech.com/most-common-causes-of-data-breaches/>
- [5] Suresh, S., Huang, H., & Kim, H. J. (2015). Scheduling in compute cloud with multiple data banks using divisible load paradigm. *Aerospace and Electronic Systems, IEEE Transactions on*, 1288-1296.
- [6] Islam, M., Islam, K., & Beg, N. (2015). Paradigm shift towards cloud computing for Banking sector. *2015 International Conference on Computer and Information Engineering (ICCIE)*, (pp. 126-129). Rajshahi: IEEE.
- [7] Goldsmith, J. (2011, 05 23). *Barclays partners with IBM for private cloud project*. Retrieved from CIO: <http://www.cio.co.uk/insight/it-strategy/barclays-partners-with-ibm-for-private-cloud-project-3431613/>
- [8] Finnegan, m. (2015, November 17). *Computer World UK*. 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/>
- [9] Gordon, W. (2012, June 20). how your passwords are stored on the internet and when your password strength doesnt matter.
- [10] Kessler, G. C. (2007). Passwords — Strengths 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. *Communication Technology (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 Computer Science and Network Technology (ICCSNT)* (pp. 972-976). Harbin, China: IEEE.
- [15] Bond, M. (2012, 09 10). *Chip and Skim: cloning EMV cards 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'a's, V., & 'R'iha, Z. (n.d). Biometric Authentication, Security and Usability.
- [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 to Determine 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.