DATA BREACHES IN INTERNET BANKING - ANALYSING THE KEY INFLUENCERS THAT IMPACT DATA VIOLATION AND ADOPTING MEASURES OF CURBING DATA VIOLATION

VISHAL DUHAN

Dept of Computer Science and Engineering,
Jaypee University of Information Technology, Waknaghat Solan(Himachal Pradesh)

ABSTRACT

In information systems, Cloud computing is a popular theme of research. 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 india. 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 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.. The advantages of using cloud computing include reduced hardware maintenance cost, easy accessibility across the globe and flexibility of highly automated processes.

Data breach is an occurrence in which touchy, secured or classified information has conceivably been seen, stolen or utilized by a person who isn't approved to do as such.

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

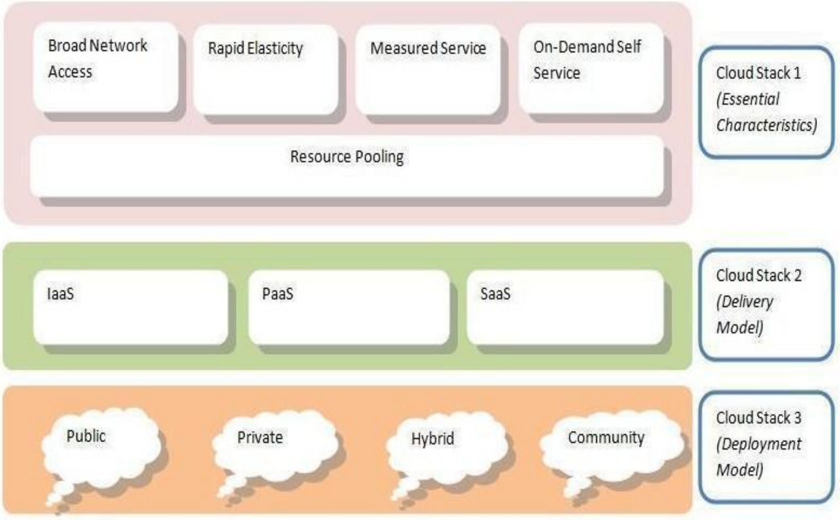


Fig 1: Architecture of Cloud computing

INTRODUCTION

In an age of globalisation and information, a ton of computing power is required to spread business bits of knowledge 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 match with quickly growing data processing requests can become very entangled 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 assures to furnish on request computing power with speedy usage, low maintenance, and less IT staff at low expenses.

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.

Cloud Computing and Internet Banking

Cloud computing basically implies the interconnected and virtualized foundations and assets that are progressively provisioned and exhibited as a artificial platform for end clients to run their applications from wherever on the planet. Banking system keeps on being delicate not surprisingly to the advance and improvement needs of the considerable number of fragments of the general public. 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 even though a survey carried out by IDC enterprise panel 74.6% of the participants identified security as the threat to adopting cloud.

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 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 infrastructure by adopting a pay as you go model with internal customer.

Authentication and Security Measures in Internet Banking

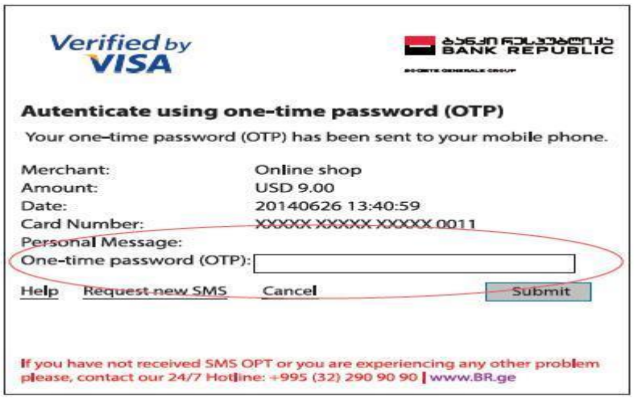
Usernames and passwords

A username is an approach to in a split second acquaint yourself with 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 substantial username connected to it, else it won't enable access to your PC, application or administration.. 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. 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. 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

One Time Password (OTP)

OTP is a code that is only valid for only a small amount of time and for only one login transaction, be it on a computer system or even digital device. OTPs contains two main variables, one is the passphrase length and other is number of times the one-time password should be hashed. It's a established fact that longer the passphrase length, better is 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.



Autenticate using one-time password (OTP)

Your one–time password (OTP) has been sent to your mobile phone.

Merchant:	Online shop
Amount:	USD 9.00
Date:	20140626 13:40:59
Card Number:	XXXXX XXXXX XXXXX 0011
Personal Message:	
One-time password (OTP):	

If you have not received SMS OPT or you are experiencing any other problem please, contact our 24/7 Hotline: +995 (32) 290 90 90 | www.BR.ge

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 . Identity authentication technology is the first protector and the portal of network system. One Time Password also faces numerous challenges like Replay attacks, Impersonation attacks and pre-play attacks.

Biometrics

Biometrics is the programmed distinguishing proof of a man in light of some physical or conduct attributes which can be fingerprint, face shape or voice. Biometrics is not used everywhere instead passwords are, nothing can be perfect and biometrics as an authentication method has its own shortcomings .

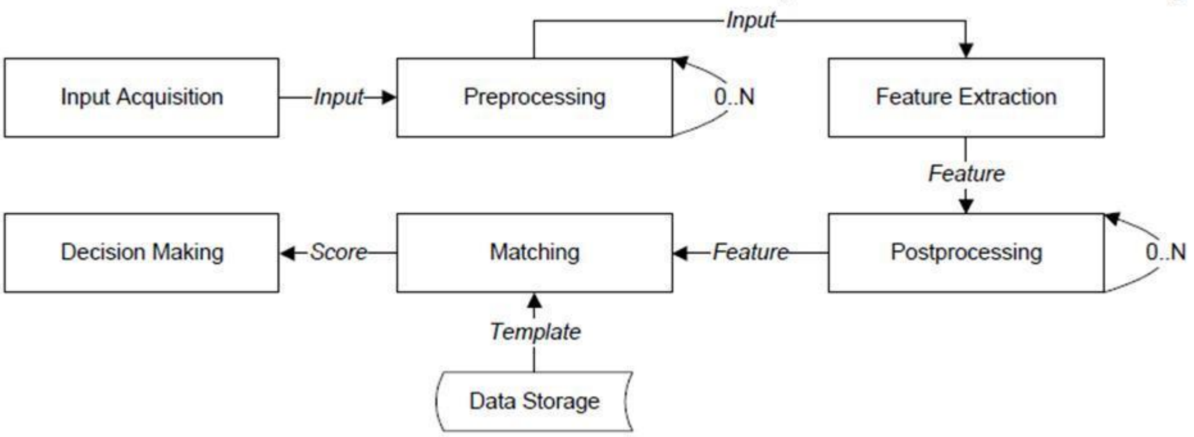


Fig 4: General Flow of Biometric System

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.

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.

RELATED WORKS

Cryptzone 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 away from unauthorized persons.

Schmidt et. al. , 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 virtualBox and Java card.
Kumar et. al., 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 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.

METHODOLOGY

Area of Study

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

Population

A descriptive survey was conducted in fifteen major banks in india 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.

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.

RESULTS AND DISCUSSIONS

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.

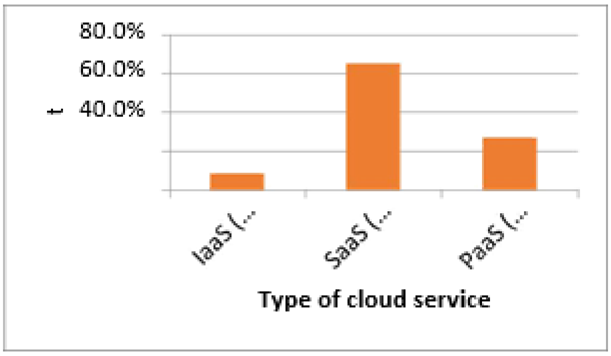


Fig 5: Cloud service models used in respondents organization

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%.

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*	*Cumulativepercentage*
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.

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 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

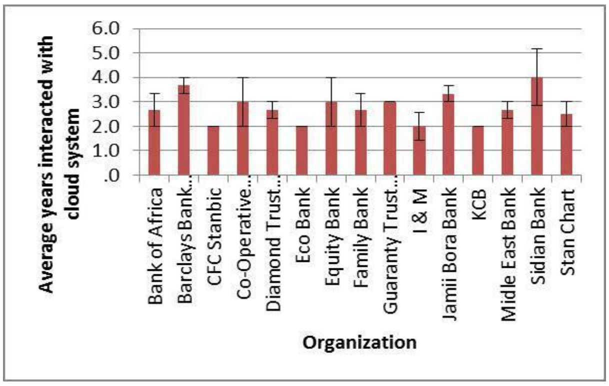


Fig 6: Duration of the Respondent Interaction with the cloud

Security Measures used

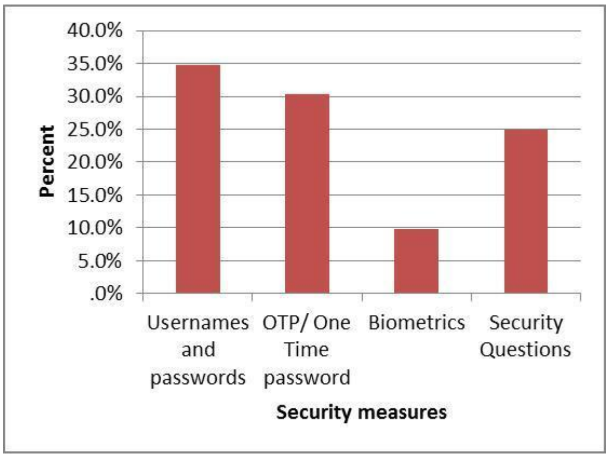


Fig 7: Security measures used by respondents' organisation

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. At 34.8%, the usage of username and passwords is most common among banks, and it is straightforwardly inverse to what others have proposed.Some affirms that the absence of standard tenets to control a client in picking of username and secret key has made it a test for clients to recollect the login certifications. OTP/One Time Password came next to username and secret key at 30.3%, this inferred a large portion of the banks were utilizing it around then of study. Biometrics recorded a low usage of 9.8% usage in security measure usage. Security Questions usage recorded a usage of 25%.

Efficiency of Security Measures

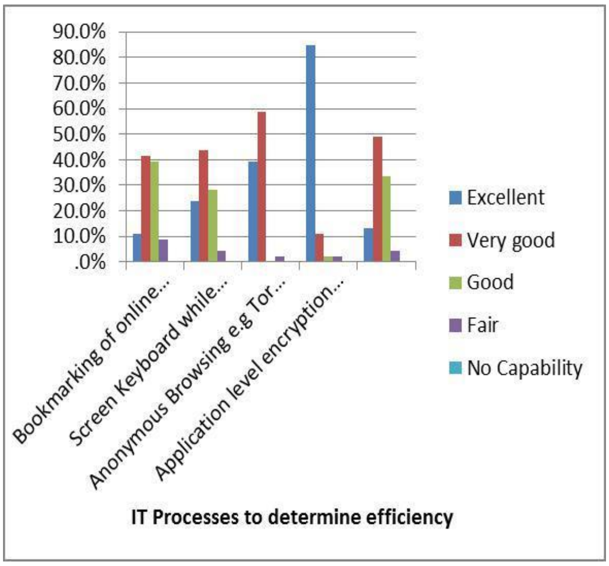


Fig 8: Efficiency of security measures

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 appraised 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% appraised it as good and almost none rated it as on no capability.

Finally on the use of established web browsers, 13.5% of the respondents appraised 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.

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.

Bookmarking

Bookmarking is saving a shortcut that directs a browser to a specific web page, 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.

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

Internet banking website login page needs to have their own on screen keyboard.

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.

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.

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.

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 assess 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.