# AN EMPIRICAL INVESTIGATION OF THE COMPUTERISED ACCOUNTING
# INFORMATION SYSTEMS FRAUDS IN LICENSED BANKS IN SRI LANKA

KENNEDY D GUNAWARDANA

Professor of Accounting Information Systems
Department of Accountancy,
University of Sri Jayewardenepura, Sri Lanka

## Abstract

*The objective of this paper is to investigate the trends in frauds of computerised accounting information systems in Sri Lankan licensed banks. Sri Lankan licensed banking sector which is the most feasible service industry contributing enormously to the growth of the country. Security controls of Computerise accounting information system in the corporate sector is taken into consideration as this is currently a growing trend around the world. The core objective is to identify the frauds in the computerised accounting information systems in licensed banks in Sri Lanka.*

*Critical reviews of past literature indicate a clear cut connection between fraud deductions in CAIS through security control systems. In order to find out the applicability of this relationship Sri Lanka, research will be undertaken in licence banks in Colombo region. The report consists secondary data which facilitate to achieve the aforementioned objectives. Secondary data analysis the existing computerized frauds in licensed banks as well as existing security control systems in licensed bank in Sri Lanka. However in secondary data analysis it clearly illustrate the computerized accounting frauds have been increased drastically. So licensed banks should have to implement the more security control systems to overcome those problems.*

**Key Words**: Computerised accounting information systems frauds, Fraud detection, Security control systems, Licensed banks.

## Introduction

Computerized accounting information systems (CAIS) are becoming more willingly available all types and size of licensed banks. With the rapid computerization of accounting using the computerised system, susceptibility to corruption, fraud and other illegal criminal activities have also increased, to banks and caused serious losses.

Computerized crimes easily happened to computerised accounting information system. It is difficult to define the computer crime. Some people may be think of the concepts such as fraud and theft. For example, sending a virus to attach a computers system, acquire funds illegally through computer, gets self-gain

using illegally obtained data files intercepting messages from third party and sending of unsolicited email or junk email.

The increase growth in real time and online data processing in CAIS had made access to these systems supplementary available and easier for many users. Therefore implementing sufficient security controls over licensed banks' CAIS and their related facilities used to handle, record, process, store and distribute information has become a necessity. The reliance's on information and continuous changes in technology force, licensed banks to implement security controls, to protect their CAIS against potential security threats.

Global spread of the internet, falling computer prices and a growing menu of applications are compelling licensed banks of every size to relay on computers to store, manage and transmit vital information. The value of this information has not escaped the consideration of hackers, cyber criminals and insiders who seek to steal from or damage on licensed banks. An irritated employee, an overzealous competitor, a probing hackers or a cyber-thief could all be sources of an attack against on licensed banking stores of computerized information. (Atul Gupta, 2003: Rex Hammond, 2004).

The high occurrence of fraud within the banking industry has become a problem to which solution must be provided in view of the large sums of money involved and its adverse implications on the economy. Frauds in its effects reduce the assets and increase the liability of any company. In the licensed banks, this may result in the loss of potential customers or crisis of confidence of banking public and in the long run end up in another failed licensed bank situation.

Although their intention may vary, individuals planning show aggression have a wide array of attack options. Erasing customer data base, planting a dangerous virus, rifling through corresponding files, sending Trojan horse, personnel records and searching for active credit card numbers are just a few of attacks that may be directed at the victim's CAIS. So all the licensed banks should be aware with the potential security threats that might challenge their CAIS and implement the relevant security controls to prevent, detect and correct such security breaches.

Currently, there is an increasing tend towards securitized control on CAIS among licensed banks in Sri Lanka. However does this system benefit Sri Lankan licensed banks in enhancing Performances? So in this, study of computerized accounting information systems frauds and security controls in licensed banks.

Many researchers identified as a computerised accounting information systems has had a significant impact on the licensed banking industry. Gunasekaran & Love, Van der smagt, (1999, 2000 cited in Mukherjee, 2003) identified that the constant development of connection over the information systems has had a significant impact on most of the commercial sectors. According to Chua & Wareham (2008), Internet auctions and computer information systems are among the most celebrated and successful new business models of the

emerging knowledge economy. However the rise of internet auctions has also led to the rise of internet auction fraud. So internet auction fraud is the most pervasive form of internet fraud. According to Chang& Bruce Ho (2006), given the vital role of IT in today's enterprises, information security has to be a key element in modern enterprise planning and management. As enterprise restrictions become blurred, security at the enterprise level becomes more challenging. Information security management (ISM) protects information from an extensive range of threats in order to make sure business continuity, minimise business damages and maximize return on investment. According to Olatunji (2009), Fraud which is the major reason for the setting up security control system, has become a great pain in the neck of many bank mangers. So they indicate that banks and other financial have further improved function as a financial intermediary by adopting diversify security control systems. The above studies conducted analyses on how security control systems have had a significant influence on the computerised accounting information systems in licensed banking industry.

## Computerised accounting information systems frauds and security control systems

The rapid change in information technology, the extensive extend of user friendly systems and the great desire of organisations to obtain and implement up to date accounting computerised systems and software have made computers much easier to be used an enable accounting tasks to be accomplished much faster and accurate than until now. On the other hand, this advance technology has also created significant risks related to ensuring the security and integrity of CAIS. (Abu Musa, 2009)

The trust of information and constant changes in technology forces an organisation to execute security controls to protect their CAIS against potential security threats. Nevertheless the failure to secure the CAIS and the information they contain or to make it accessible when it is required can, and does, lead to great financial and non-financial losses. (Abu Musa, 2007)

Gupta & Hammond (2005) pointed it, Security surveys have specified a few trends that are emerging in various locations around the world. In Australia, surveys indicate poor level of computer security among the countries' businesses, owed to poor security measures and implementation. It is estimated that 45% of organisations did not budget for computer security. In the UK, 42%, of organisations did not have an information security policy and 49% organisations listed budget constraints as being the primary issue in implementing computer security.

Information technology has become part and partial of the banking sector world today. In fact, it will continue becoming an ever large factor in the future. Banking sector will interlink their IT systems as a result of linking to the internet, electronic data interchange (EDI), etc. All of this might hold an information security risk for an organisation as well as banking sector.

Organisations attempt to secure their own IT environment, however they have little control over the IT systems they link with. If those environments are insecure, they might pose a threat to the IT systems in the host environment. (Technikonv et al, 1998).

Increased organisational dependents on Information system (IS) has led to a corresponding increase in the impact of CAIS security abuses. While such a trend would suggest IS security as a key management issue, this has not been the case in practice. Management attention for CAIS security has been low compared to other IS issues. (Kankanhalii et al, 2003)

## Existing level of financial frauds in licensed banks

According to Metrejean, et al (2005) pointed that, the computer security institute (CSI) and Federal Bureau Investigation (FBI) examination encompasses respondents from many organisations from many different industries. This report shows the types of computer crimes, the technological used to prevent the crimes, the number of attacks and the dollar amount of losses by type of attacks. The 2003 report show that the number of attacks was about the same in 2001 and 2002, but the financial losses caused by the attacks declined by approximately 56% from 2001 to 2002. The report showed that losses declined in areas such as theft of proprietary information and viruses, but increased in areas such as denial of service attacks, unauthorised access, and sabotage. (Metrejean, et.al, 2005)

According to Idowu & Abiola mentioned that money transfer services are means of moving to or from a bank to beneficiary account at any bank point worldwide in accordance with the instructions from the banks' customers. Some common mean of money transfer are mail, telephone, over the electronic process and telex. Fraudulent money transfer may result from a request created solely for the purpose of committing a fraud or altered by changing the beneficiary's name or account number or changing the amount of the transfer.

Every day, reports can be found in accounting and financial publications about computer related data errors, incorrect financial information, violation of internal control, thefts, burglaries, fires and sabotage. Organisations should be aware with the potential security threats that might challenge their CAIS and implement the relevant security controls to prevent, detract and correct such security breaches. (Abu Musa, 2008)

According to Ballerini & Beckers (2003) pointed out report by the US federal trade commission (FTC), national and state trends in frauds and identify theft shows that during the year 2002 to 2003 internet fraud related complaints rose continuously, in both numbers and percentages of all fraud complaints in banks. By 2003 internet related fraud complaints accounted for 47% of 218, 284 complaints filed with the FTC.

One form of data manipulation, called data diddling, involves changing data within a database. Data manipulation includes adding, deleting or altering data within the database. Generally, such manipulation is perpetrated by an employee of the organisation and is aimed at changing the financial data. Changing financial data results in incorrect financial statements or other financial reports that many individuals, both internal and external, use to make important decisions. (Metrejean, et al, 2005)

According to Adams clearly outline that retrospective to each payment or loyalty transaction data is screened using client and sector specific rules to distinguish whether any unusual activity has occurred. This can highlight internal fraud, including collusion between employees, "sweetheart" fraud and abuse of staff discount and loyalty cards. For example, if the same loyalty card keeps being applied to multiple transactions, this could indicate that an employee is collecting loyalty points for themselves rather than applying them to the legitimate customer.

The growth of digital/computer technology procreates fraud and generates additional risks of swindling and illicit activities in the future. The internet can be used in crimes ranging from simple extortion to the most complicated, transactional effort. A dissection of fraud involving the internet revealed three major categories: securities fraud, fraud in electronic commerce and fraud from internet companies. (Seetharaman, et.al, 2004)

A number of current techniques for obtaining customers' personal data may not even necessitate or effective breach of the bank's security measures. To yield customer data online, fraudsters frequently establish so called "spoof sites": Websites that they have created using the HTML code of genuine banks' sites. By sending e mails with false information (Such as reports of security or technical problems) to the legitimate Banks customers' the frauds can scam the customers into entering large amounts of valuable personal data, then those data to access existing financial amounts of valuable personal data, then use those data to access existing financial accounts or establish new accounts. Some of the largest and most extensively recognized banks in the USA such as bank of America, AT & T Bank have been target of spoof sites. (Ballerini & Beckers, 2003)

## Computerized accounting frauds and security controls in Sri Lankan licensed banks

Computerized accounting information systems (CAIS) are becoming more willingly available all types and size of licensed banks. The increase growth in real time and online data processing in CAIS had made access to these systems supplementary available and easier for many users. With the rapid change in utilization of Computerized Accounting Information Systems in licensed banking sector, especially in Sri Lanka, security controls of CAIS's have become very widely spoken and widely visible topic in the licensed banking sector. Licensed banks are justifiably concern to detect frauds. And also currently in licensed banks volume of banking transactions are rapidly increasing. As a result computerized accounting frauds are also escalating.

### Volume of computerized banking transactions

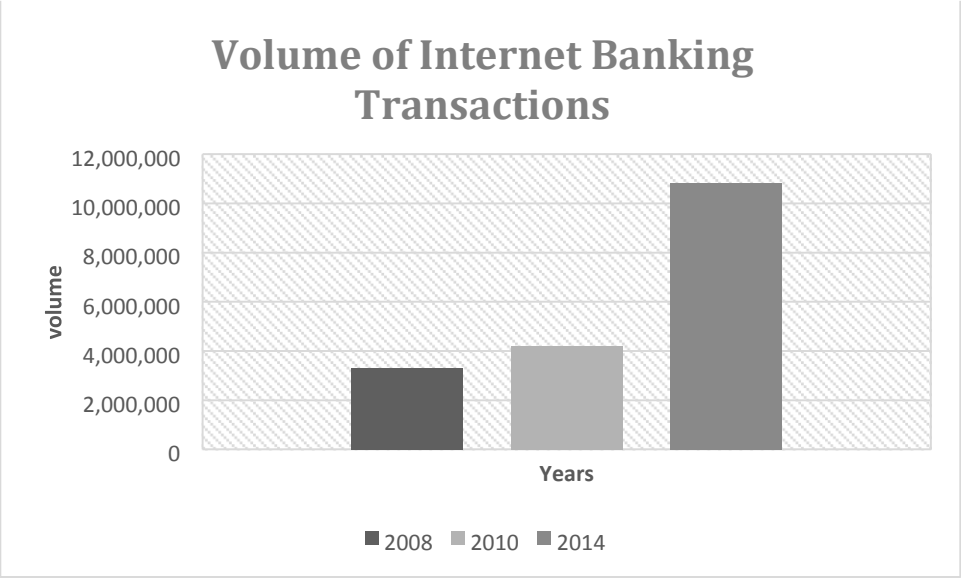


**Figure 1: Volume of Internet banking transactions**
Sources: Central bank of Sri Lanka, (2014)

With technological advancements in the banking system and introduction of new fund transfer means and payment systems through computerized have made customers to tend to use more electronic payment methods in comparison to conventional banking methods (CBSL, 2010).The central bank of Sri Lanka depicted in its annual report that the volume of computerized accounting banking transactions have increased from 3,310,000 to 3,819,000 which depict an increase of 13.32%. Therefore CBSL has adopted security measures to strengthen the payment systems and minimize all risks involved in improving the soundness of the financial systems. According to above figures volume of the internet banking transactions are speedily increasing in the licensed banks.

## Value of internet banking transaction

In Sri Lanka most of the licensed banks are offer financial services via the internet and also value added services customers do not normally enjoy at the banking counters in the most customers friendly manner. As a result in most of the Sri Lankan licensed banks value of internet banking transactions are going increases. It can be shown as follows,

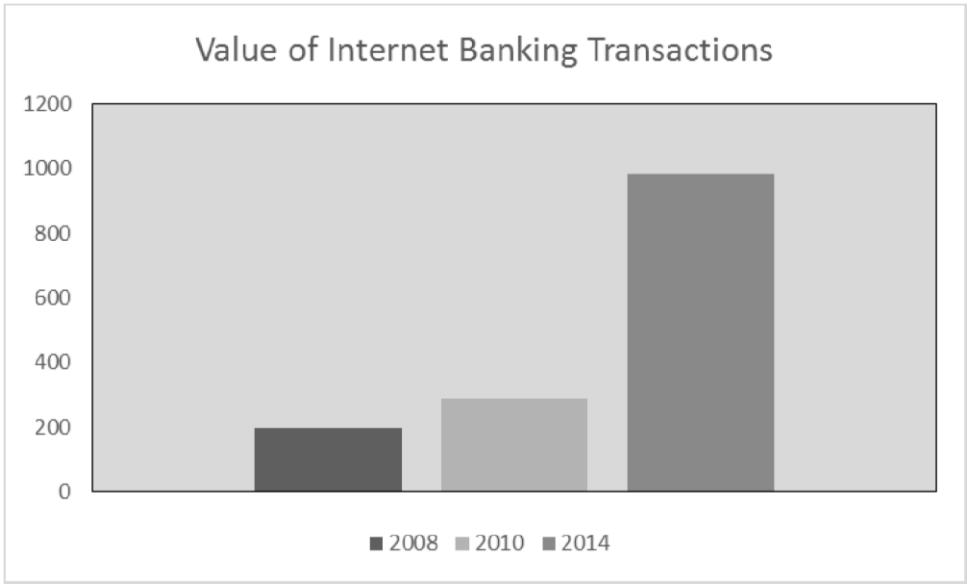


**Figure 2: Value of internet banking transactions**
Sources: Central bank of Sri Lanka, (2014)

Central Bank of Sri Lanka in its annual report in 2009 portrayed an increase of the value of computer accounting banking transactions which took place. The value had a significant increase from 197 Billion rupees to 247 Billion rupees which showed a hike of 25.4%.and also in 2009 to 2010 value of computer accounting banking transactions are increase by 16.5% Therefore CBSL is taking steps in order to set up a more secured environment for transactions and settlements of electronic payments as there has been an increase due to the developments in ICT technology and the increase of preference of people to use such modes for their transactions therefore in order to build public confidence on electronic payments CBSL is strengthening the security systems.

## Computerized accounting Banking Frauds Incident reports (SLCERT)

Sri Lanka Computer Emergency Response Team (SLCERT) which is the centre for cyber security in Sri Lanka is authorized to protect the state's information infrastructure and to synchronize protective measures against cyber-crimes, security threats and vulnerabilities. According to SLCERT, (2010) incident computerized accounting banking frauds are can be demonstrate as follows,

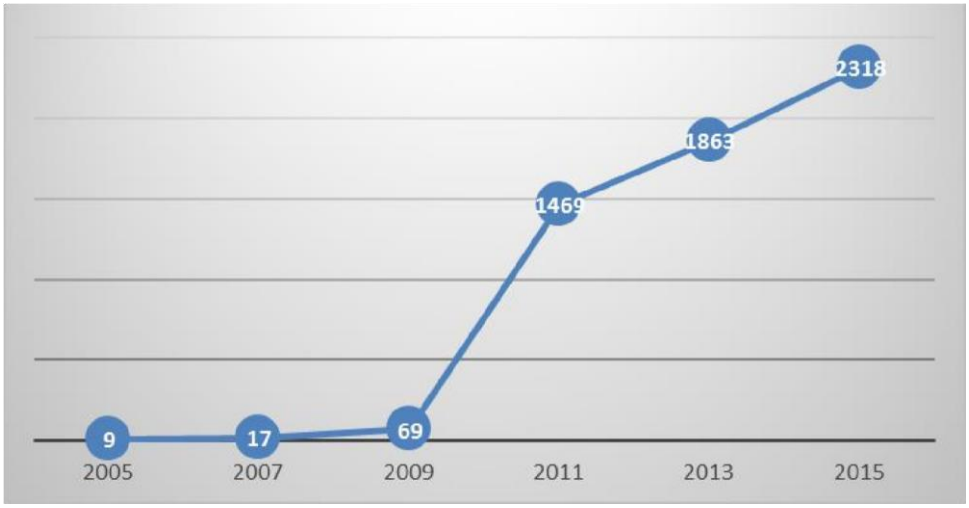


**Figure 3: Computerized accounting banking frauds incident reports**
Sources: SLCERT: (2014)

The incidents reported to SLCERT has rapidly increased from the year 2005 to 2010 which demonstrates as the value of the computer accounting banking transactions are increasing the incidents reported to have seen a significant increase. According to SLCERT data, incident frauds are increasing drastically in 2005 to 2008, nevertheless in 2009 to 2010 incident reports are slightly decreasing. Because, of most of the licensed banks are extremely focusing on their computerized security control systems to dropping computerized frauds. However, these data are only reported to the SLECERT, so we could not come to a conclusion in 2009 to 2010 computerized accounting frauds are reducing in licensed banks.

And also the Sri Lankan government has introduced a new act titled Computer Crimes Act in 2007 to curtail electronic crimes in Sri Lanka.

SLCERT has worked hard in order to resolve all cases reported to it satisfactorily. These incidents represent the way internet banking frauds occur which violates the trust the customers have towards the bank therefore sound security measures have been implemented in order to rectify these issues occurring.

## Bank frauds reported statistics

While developments in the area of information technology have resulted in benefits such as anywhere, anytime, banking a disturbing factor has been the rising incidents of preparation of computerized accounting frauds. Frauds in complicity with bank staff in emerging areas and services under the computerized environment. (Business line, 2010)

So there are some of computerized frauds in licensed banks reported to the CID and SLECRT. It can be explain as follows,

| **Type of fraud** | **No of frauds** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **2005** | **2006** | **2007** | **2008** | **2009** | **2010** | **2014** |
| Credit card frauds | 18 | 23 | 25 | 31 | 39 | 45 | 132 |
| ATM card frauds | 7 | 9 | 14 | 19 | 22 | 25 | 251 |
| Falsification of accounts (bank accounts recorded in incorrect) | 24 | 27 | 29 | 33 | 37 | 41 | 411 |
| Dormant accounts fraud (Using Dormant accounts and cash transferring to fake account accounts through computer) | 8 | 11 | 13 | 17 | 19 | 22 | 223 |
| System hacking | 7 | 11 | 15 | 19 | 21 | 24 | 240 |
| Password tracking | 7 | 16 | 19 | 23 | 28 | 34 | 314 |
| Network frauds | 5 | 8 | 10 | 13 | 16 | 19 | 219 |
| Entry in to system of computer viruses and worms | 6 | 8 | 11 | 13 | 16 | 19 | 419 |

**Table 1: Bank frauds reports statistics**

Sources: CID, (2014)

## Credit cards

According to Central bank of Sri Lanka, (2010) mentioned that the total number of number of credit cards in use was 892,291 at the end of March 2010, showing a decrease of 4% over that of end December 2009.The total number of new cards issued under all categories during the quarter dropped substantially by 35% to 20,615 when compared with first quarter of 2010. Adverse economic conditions and mainly security threats may have the cause for the decline.

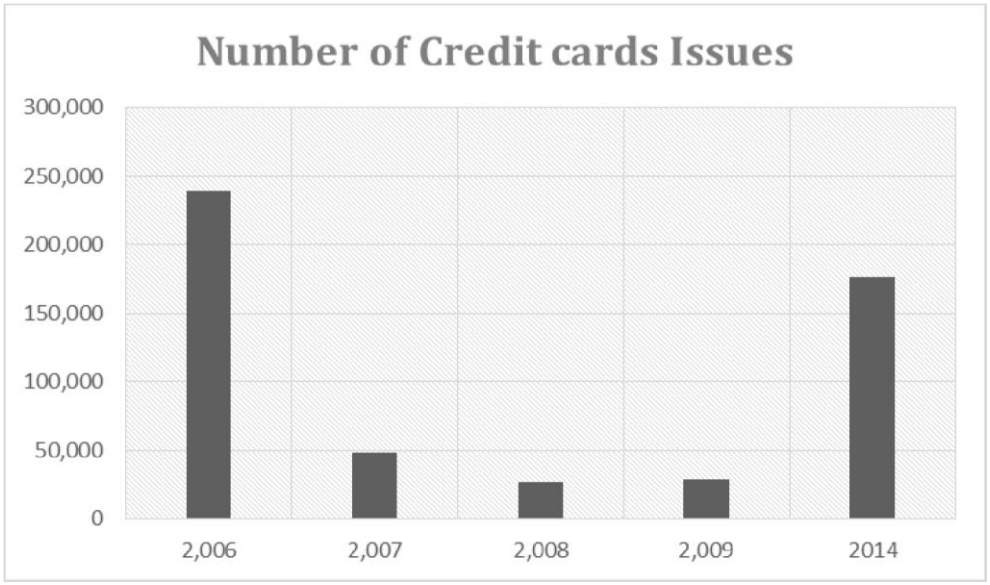


**Figure 4: Total number of new credit card issues**
Sources: Central bank Annual report, (2014)

According to Central bank of Sri Lanka,(2010) mentioned that the total number of credit card transactions declined by 7% to 4.4 million and the total value of credit card transactions decreased by 10.3% to Rs. 15.7 billion in the first quarter of 2009, when compared with those of the previous year. These declines were attributed to the drop recorded in number of domestic cards in use by 34% during the first quarter 2009.

**No of transactions per credit card**

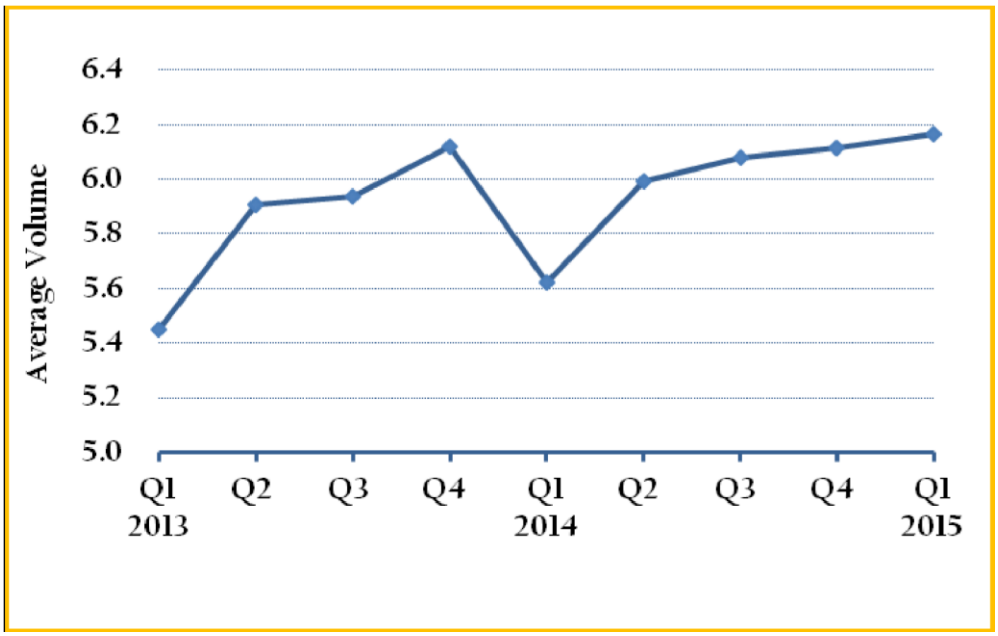


**Figure 5: No of transactions per credit card**
Sources: Central bank Annual report, (2014)

According to above chart shows the declining trend of the number of transactions per credit cards. In the first quarter 2009 number of transactions per credit cards dropped to 5.3m from 5m recorded in the first quarter of the 2008. High security threats of the computerized systems could be attributed reason for above trend.

## Credit cards frauds incidents reports

If a fraudster has simply attained a credit card's details, either by coping the details down during a transaction or by interrupting the details through the internet, it is possible for them to make unauthorized purchases online. If a criminal has obtained sensitive bank details, through phishing or e commerce scams for instance, they may find it possible to illegally hijack and abuse the victim's accounts. If the fraudster has gained access to a bank account it may be possible for them to change passwords, blocking out the victim, and empty the account into another temporary account to withdraw the funds. (Savings.com, 2010)

According to CRIB reports number of credit card frauds incidents are rapidly increasing during 2005 to 2010.It can be show as follows,

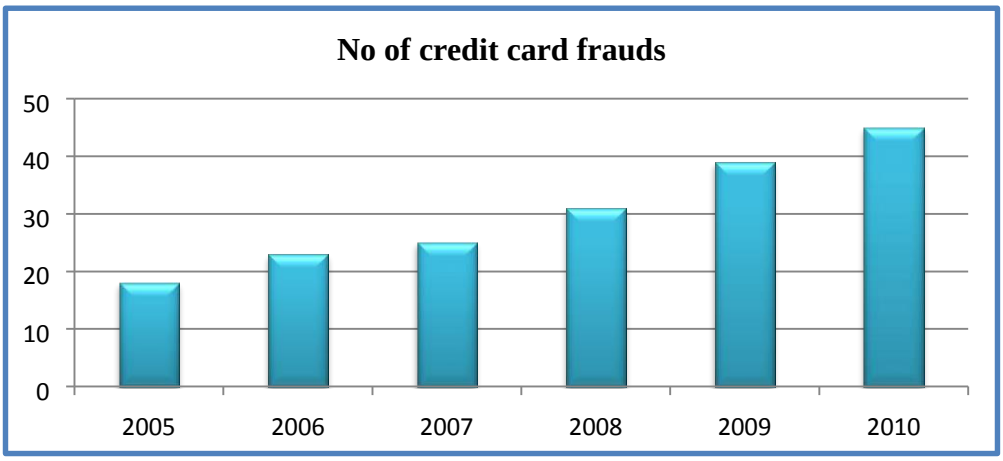


**Figure 6: Number of credit cards frauds**
Sources: CRIB, (2010)

The incidents reported to CRIB has rapidly increased from the year 2005 to 2010 which demonstrates as the volume of the **credit card frauds** are increasing the incidents reported to have seen a significant increase. Credit cards also handling by through computerized system. Base year is the 2005.

According to above table, mentioned that the credit card frauds incidents cases are percentage vies. So it clearly shows that the declining the percentages by year to year. However number of credit cards frauds has been increased. As a result we can clearly considerate the credit card transactions are dramatically declined by year 2005 to 2010 due to the high security threats of credit cards by using computerized information systems.

**ATM Terminals**

| | First quarter | | |
|---|---|---|---|
| | **2014** | **2015** | **2014** |
| Total volume of financial transactions | 23.6 m | 24.5 m. estimate | 3.8% |
| Total value of transactions | 134.6 B | 154. 5 B estimate | 1.4% |

Sources: Central Bank of Sri Lanka, (2015)

According to above table, total volume of transactions through ATM had been increased by 3.8% percentage with compared to 2014 to 2015. And also total value of transactions had been increased, however value of transactions increased percentage is when compared with 2014 to 2015 is relatively low percentage. The adverse economic conditions and mainly security threats may have the cause for the decline.

### ATM Card frauds incident reports

ATM scams are becoming increasingly widespread because criminals are employing hi tech methods to hack into customers bank accounts. ATM frauds are on the rise, law enforcement officials say, because thieves are becoming more and more sophisticated. Criminals have become very clever at finding new ways to access your funds so consumers need to pay careful attention to their bank statement in case there are unauthorized withdraws because it's more likely that someone has access to your bank account information. (Bustathief.com, 2010)

According to CID reports number of ATM cards frauds can be graphically illustrate as follows,

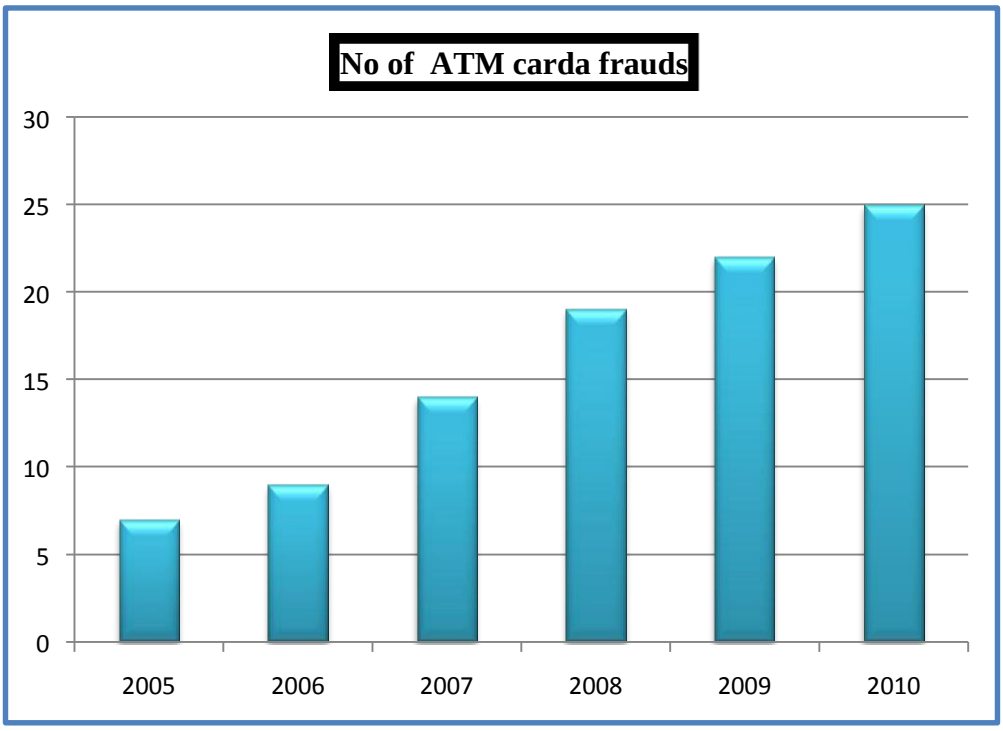


**Figure 7: Number of ATM card frauds**
Sources: CID, (2010)

According to CRIB reports, an ATM card fraud has rapidly increased. Mainly HSBC Bank and Commercial bank as well as Nations trust bank reported to CRIB has increased. ATM machine controlling by through computerized system and ATM card frauds mainly happened in get serial number of the card and enter to the system.

## Falsification accounts frauds incident reports

All of the licensed banks are today accounting transactions are recorded to ledger accounts through computer system. So according to CID reports, when recording bank transactions, some employees are recording the transactions are incorrect account. So like that frauds also increased in 2005 to 2010. It can be shown as follows,

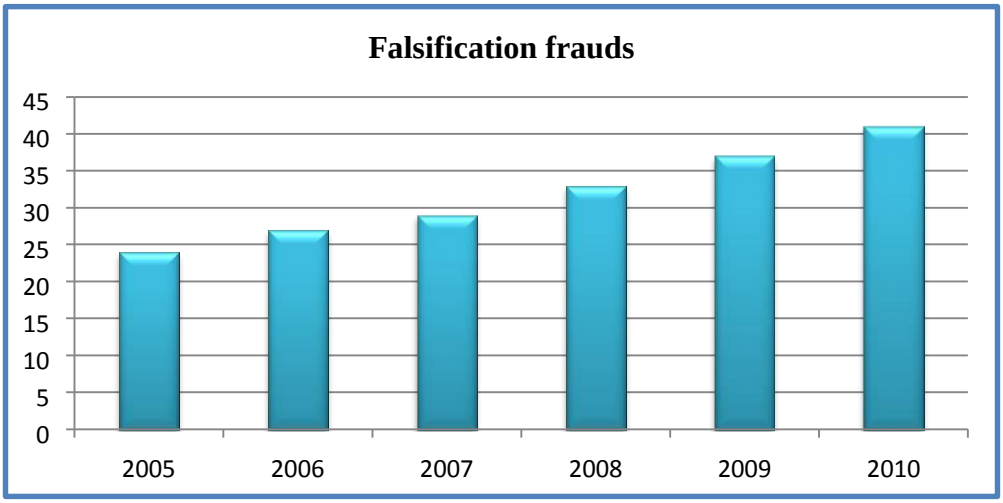


**Figure 8: Number of Falsification frauds**
Sources: CID, (2010)

According to above calculation, Falsification computerized accounting frauds increasing percentage evaluated with 2005 to 2006 increased by 12.5%, and 2007 increased by 7.4% again 2008 increased 13.7%.Again 2009 and 2010 relatively 12.12% and 10.8%. So Falsification computerized accounting number of frauds are increasing, however as a percentage it has been changed in year to year.

## Dormant accounts frauds

According to CID reports, they reported Dormant accounting frauds in licensed banks also. It can be happened in; using Dormant accounts names and money transferring to fake account. It is also a major fraud in the banking system. This is done by using computer system in the banks. This is mainly happened in used migrated customers' bank accounts. It can be graphically illustrate as follows,

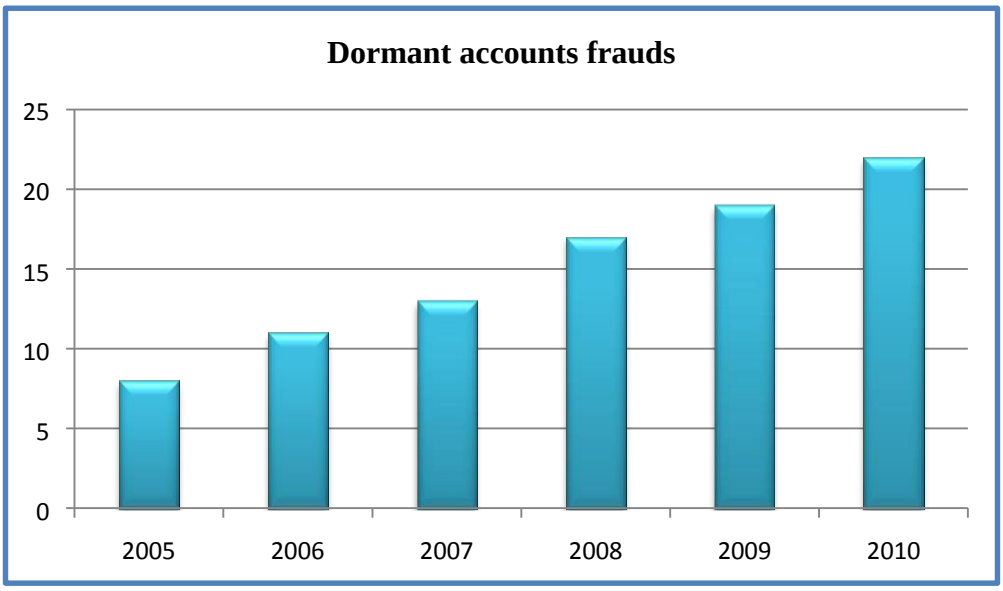


**Figure 9: Dormant accounts frauds**

Sources: CID, (2010)

According to above calculation, evidently discovered the Dormant accounting frauds increasing as a percentage. With compared to 2005 to 2006 increasing percentage is 37.5% as well as 2007 and 2008 relatively 18.18% and 30.76%. So Dormant accounts frauds have been increased as a number of incidents wise.

## System hacking frauds

The incidents reported to CID has rapidly increased from the year 2005 to 2010 which demonstrates as the volume of the system hacking and doing computer frauds are increasing the incidents reported to have seen a significant increase. They hacking the banking security system and done by

frauds. Number of system hacking frauds can be shown as follows.

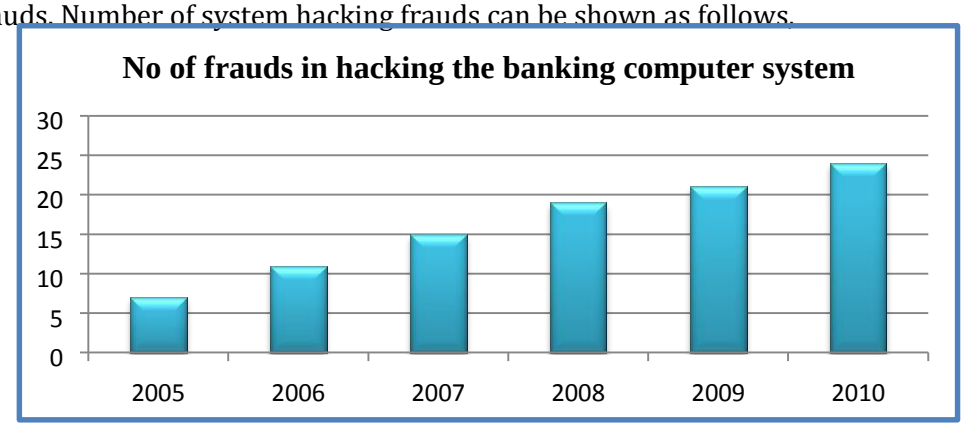


**Figure 10 number of Systems hacking frauds**

Sources: CID, (2010)

According to above calculation evidently discovered the system hacking frauds increasing as a percentage. With compared to 2005 to 2006 increasing percentage is 9.09% as well as in 2006 to 2007 the system hacking frauds increasing as 17.54%. As similar in 2008, 2009 constantly increasing the systems hacking continually 37.89% as well as 54.67%.

## Password tracking frauds incident reports

The incidents reported to CID has rapidly increased from the year 2005 to 2010 which demonstrates as the volume of the computer password tracking are increasing the incidents reported to have seen a significant increase. This type of frauds mainly had in the Nation trust bank as well as Bank of Ceylon bank. According CID reports number of password tracking frauds incidents can be illustrate as follows,

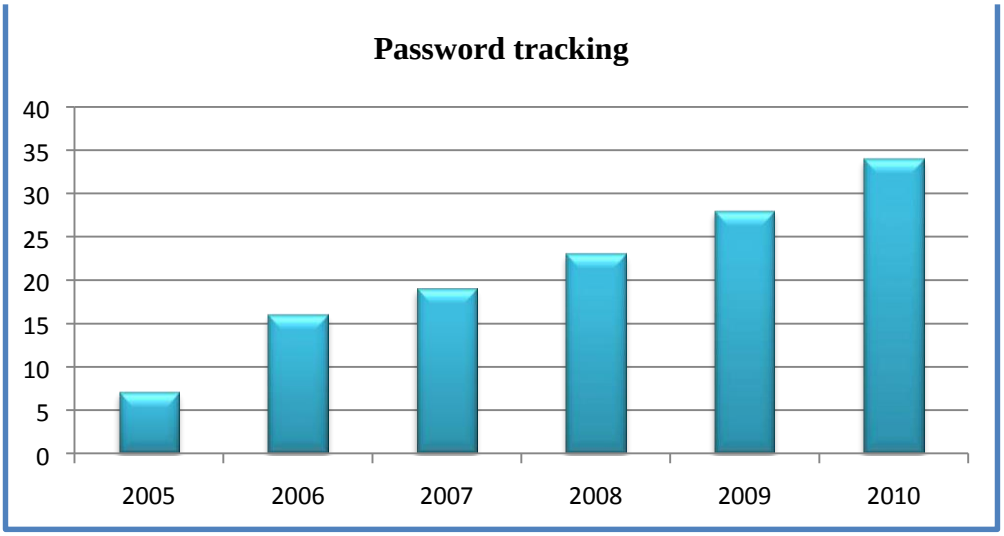


**Figure 11: Number of password tracking frauds**

Sources: CID, (2010)

According to above calculation clearly illustrate the password tracking frauds incidents reports are going increasing. As a percentage in year 2005 to 2006 by 24.65% increasing password tracking frauds. And same as in year 2007 32.87% and 34.67% pass word tracking frauds are increasing. According to this data clearly illustrate when the banks computerized usage are increasing constantly password tracking frauds also increase.

## Network Frauds

Network frauds mean, in banking system when enter the transactions for customer accounts through computerized system, creating the separate account and when transactions are entering to the system, each transaction some amount go to the created account. It could be done in entering to the banking security system and hacking their network connection. This type of fraud cases were reported to the CID. This is drastically increased in year 2005

to 2010, because of escalating advance information technology. Number of network frauds can be shown as follows,

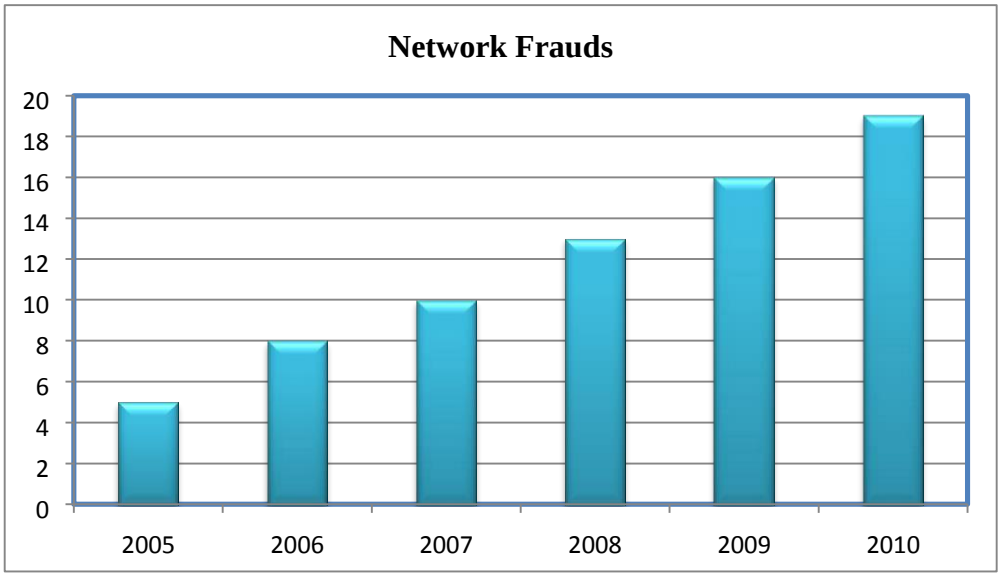


**Figure 12: Number of network frauds**

Sources: CID, (2010)

According to the above data clearly illustrates the how much percentages increase by network frauds in each year. In 2005 to 2006 network frauds increased by 13.5% as well as 23.75% in year 2007. In year 2008 network frauds increasing by 28.65% and in year 2009 that was increased by 32.45%. According to above data network frauds increased by in each year.

### Entry in to system of computer viruses and worms

Recently banks are facing very serious problem is an entry in viruses of computer systems. So this type of frauds cases was reported to the SLECRT. The result of this mainly indicated most of the Sri Lankan licensed banks were less prepared and had taken fewer measures to protect against potential security threats in like as viruses and worms. According to SLECRT reports only 45-50% licensed banks secured their accounting systems from viruses by using secure systems. So entry in to system of computer viruses and worms frauds can be illustrate as follows,

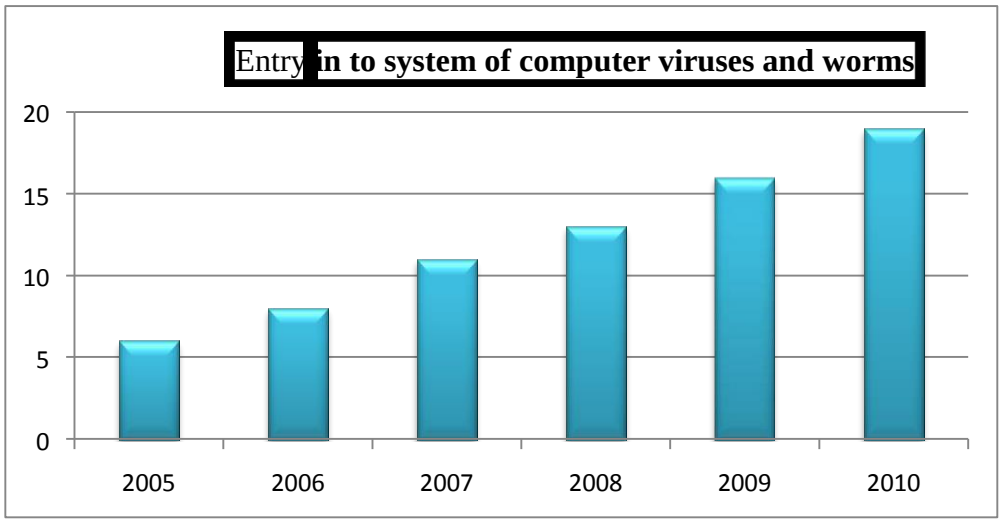


**Figure 13: Entry in to systems of computer viruses and worms**

Sources: SLCERT, (2010)

According to the above data clearly outline the entry in to systems of computer viruses and worms are increasing constantly. In year 2005 to 2006 increased by 12.56% as well as in 2006 to 2007 increased by 17.57%.In 2008 and 2009 and 2010 also constantly increasing the computer viruses and worms in to the systems.

## Conclusion

As computerized accounting information systems are still progress of growth but sometimes not acceptable to quite an extent by security, delivery, authenticity and accessibility to overcome this issues licensed banks are using computerized accounting security control systems to overcome these problems.

The secondary data analysis has mainly been conducted to identify the existing computerized accounting frauds happened in licensed banks in Sri Lanka and also existing security control systems in licensed banks. However in secondary data analysis it clearly illustrate the computerized accounting frauds have been increased drastically. So licensed banks should have to implement the more security control systems to overcome those problems.

In Sri Lanka to reduce the computerized accounting frauds have not been given much significant attention because of if the banks are using high security control systems to the protecting a physical environment than computerized systems, then customers are not satisfied with those security rules and regulations, because sometime if implementing high security breaches then customers have to willing more time to do the transactions. However, Sri Lankan licensed banks have to give more attention to computerized fraud detection security control systems.

## References


Abu Musa, A.A. (2009). *Exploring the perceive threats of computerized accounting information systems in emerging countries: An empirical study of Saudi organizations*. Department of Accounting & MIS KFUPM, Saudi Arabia Vol.21.No 4.pg. 387-407

Abu Musa, A.A. (2008). *Information technology and its implications for internal auditing an empirical study of Saudi organizations*. Department of Accounting and MIS, Saudi Arabia. Vol. 23, No.5. pg. 438-466

Abu Musa, A.A. (2007). *Evaluating the security controls of CAIS in developing countries: an examination of current research*. Department of Accounting & MIS, College of Industrial management, King Fahd University of petroleum's & Minerals, Dhahran, Saudi Arabia.Vol.15.No 1.pg.46-63

Abu Musa, A.A. (2004). *Investigating the security controls of CAIS in an emerging economy: An empirical study of the Egyptian banking industry.* Department of Accounting & MIS, College of Industrial management, King Fahd University of petroleum's & Minerals, Dhahran, Saudi Arabia. Vol. 19 No. 2. Pg.272-302

Adams, R, (2010). *Prevent, protect, purse- a paradigm for fighting fraud*. Computer fraud security international journal (2010) pg. 4-10

Anon, (2001) *Information system audit policy for the banking and financial sector.* Department of information technology Preserver bank of India Mumbai (2001) Pg.3- 7

Bierstaker, J.L, Brody, R.G. & Pacini, C. (2006). *Accountants' perceptions regarding fraud detections and prevention methods.* Department of Accountancy and finance, college of commerce and finance, Villanova University, Villanova, Pennsylvania, USA. Vol. 21.No.5. Pg.520- 535

Business line, (2010). *Bank frauds reports* [Online] Available: http://www.hinduonnet.com/businessline/2001/07/23/stories/042308ju.htm [Accessed on 20th February 2011]

Bustathief.com, (2010). *ATM Machine fraud –cashpoint scam* [Online] Available: http://www.bustathief.com/atm-fraud-or-cash-money-theft-is-as-old [Accessed on 1st of March 2011]

CBSL Annual Report, (2009). [Online] Available: http://www.cbsl.gov.lk/pics_n_docs/10_pub/_docs/efr/annual_report/ar2009_e/PDF/13_Part_02.pdf [Accessed on 12th October 2010]

Cansec systems ltd, (2009). *Access control systems for a more secure future* [Online] Available: http://www.cansec.com/ [Accessed on 20th March 2011]

Central bank of Sri Lanka, (2009*). Economic outlook and policy measure* [Online] Available:

[www.cbsl.gov.lk/pics_n.../10.../**payment**.../**Payments** Bulletin_4Q08.pdf [Accessed on 15th February 2011]

Chu, C.E.H. & Wareham, J. (2008). *Parasitism and Internet Auction Fraud; An exploration.* International journal of information and organization (2008) Pg.303-333

Database security guide, (2010). *Security checklists and recommendations* [Online] Available: http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/checklis.htm [Accessed on 23rd March 2011]

Ezine Market.com, (2010). Access control and card entry security systems [Online] Available: http://technology.ezinemark.com/access-control-and-cardentry-security-systems-31c52393e96.html [Accessed on 3rd of March 2011]

Gunasekaran & Love, 1999 A. Gunasekaran and P.D.Love, *current and future applications of multimedia technology in business.* International journal of Information Management 9 (1999), pg. 5-121.

Gunatunge, R.S.2003. *Habermasian way of understanding information systems development in organizations in Sri Lanka*. 9th International conference on Sri Lankan studies full paper number 106 (2003)

Gunawardana, K.D. & Rajeshwaran, N. (2007). *An empirical investigation of the security controls of computerized accounting information systems (CAIS) in the selected list companies in Sri Lanka*.

Gupta, A. & Hammond, R. (2005).*Information systems security issues and decisions for small businesses: An empirical examination*. School of business and economics, Lynchburg College, Lynchburg, Virginia, USA. Vol. 13.No.4. pg. 297310

Gordan, L.A, Loeb, M.P & Lucyshyn, W. (2003). *Sharing information on computer systems security: An economic analysis*. Journal of accounting and public policy. Pg.461-485

Idowu & Abiola, (2009). *An assessment of fraud and its management in Nigerian commercial banks* European journal of social science Vol.10, Pg.632-635

Kankanhalii, A., Teo, H.H, Tan, B.C.Y & Wei, K.K. (2003). *An integrative study of information system security* effectiveness. International journal of Information Management. No23.Pg. 139-154

Metrejean, E, Smith, H.G, & Elam, D. (2005). *Educating accounting students on computer crime and ethics.* Journal of business and economic research. (2005)Vol.3. No. 9.pg. 77-88

Munir, U & Manarvi, (2010). *Information security assessment for banking sector –A case study of Pakistani Bank.* Global journal of computer science and technology, Vol. 10 pg.44

Olatunji, O.C.(2009). *Impact on internal control system in Banking sector in Nigeria*. Pakistan Journal of social science (2009) Pg.181-189

Reference for business, (2010) *Computer security,* [Online] Available: http://www.referenceforbusiness.com/encyclopedia/Clo-Con/ComputerSecurity.html [Accessed on 25th march 2011]

Sekaran, U. (2003).*Research Methods for business: A skill building approach*, 4th Ed, Kundli, John Wiley & Sons.

Setharaman, A, Senthilvelmurugan, M & Periyanayagam. (2004). *Anatomy of computer accounting frauds.* Faculty of Management multimedia university, Malaysia. Vol.19. No. 8.Pg. 1055-172

Senivirathna, N, (2008). *Rising to the challenges: Can internal auditors play a strategic role in turbulent times?* Journal Of commercial Bank Qatar (2008) pg.185 -188

Savings.com,(2010). *Credit cards frauds how identify thief's use your information* [Online] Available:http://www.savings.com/blog/post/Credit-Card-FraudHow-Identity-Thiefs-Use-Your-Information.html [Accessed on 23rd February 2011]

Technikon, E.P. & Elizebeth,P. (1998). *Information Security management (1): Why information security is so important.* International journal of information Management (1998).

Zhu,D,(2002). *Security control in internet bank fund transfer*. Journal of electronic commerce research (2002) Vol. 3,No,