U- COMMERCE AND ITS IMPACTS IN E- BANKING SECURITY ISSUES

Dr. B. GAYATHRI, M.Com, M.Phil, PGDCA, Ph.D.,
ASSISTANT PROFESSOR
DEPARTMENT OF COMMERCE
PSG COLLEGE OF ARTS &SCIENCE
COIMBATORE
gayabalu22@gmail.com
9442754371

ABSTRACT

To elaborates and extends several new concepts that lay the foundation for thinking about next-generation commerce called U-Commerce or Ultimate Commerce. As the technology shifts from traditional to electronic, electronic to mobile the way of commerce is also changed. But apart from all of these technologies and advancement another emerging field of wireless communication called as U-Commerce.

U- Commerce is abbreviation that stands for ubiquitous commerce, also called ultimate commerce. Ubiquitous networks which can be accessed at "any time form any place "and using a range of devices are base of new kind of commerce. U-Commerce is combination of E-commerce, M-commerce, television, voice and silent commerce.

Electronic commerce has emerged, allowing business to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The e-banking system addresses several emerging trends: customers demand for anytime, anywhere service, while e-banking has improved banks efficiency and convenience, like technology service providers globally have firmed up cloud computing platforms that have opened views for alert and cost effective solutions. Prevention of cyber crimes is the main challenge for banks with proper customer service

People today prefer using electronic medium for banking because of lot of advantages associated with it. Though e-banking provides lot of advantages in form of speed, ease and convenience it has also put forth some issues and challenges that needs to be addressed. In this paper, an attempt has been made to give an overview of e-banking, how it has evolved over a period of time in India.

Keywords: U-commerce, m-commerce, e-commerce, Ubiquity, Universality
E-Banking Functions, E-banking security, privacy, E-banking in India.

INTRODUCTION

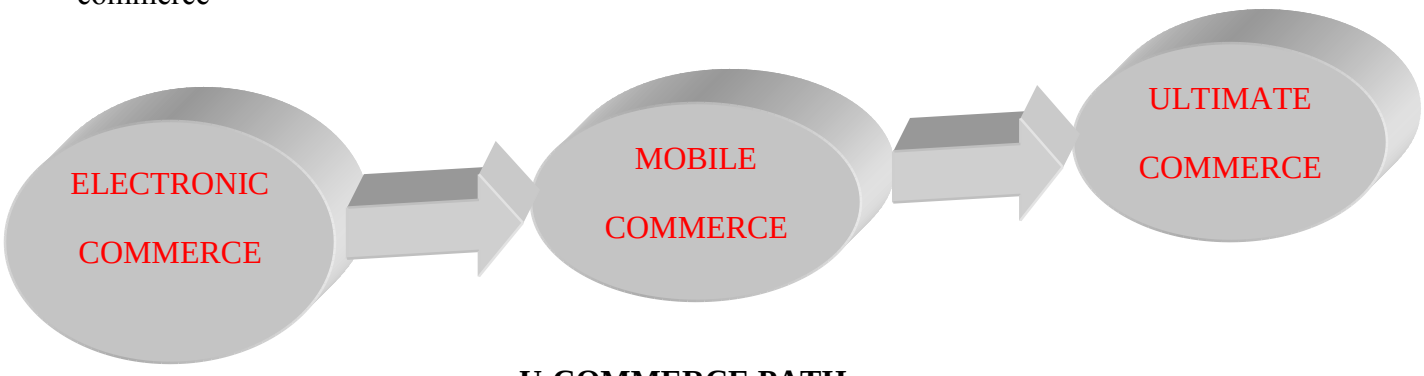
Commerce means buying and selling or the exchange on a large scale and includes marketing activities like standardization, grading, packing, storing and transportation from one place to another. Until now we know some of the following types of commerce.

- E - Commerce: - Most popular, doing transaction on Internet
- M - Commerce: - Business transactions through mobile
- V - Commerce: - Using voice commands to do transactions
- P - Commerce: - Proximity commerce using Bluetooth technology

Electronic commerce has hit the business world like a tremendous change over the past several years, first with a wave of excitement around business-to-consumer (B2C), and then business-to-business (B2B) and person-to-person (P2P). All of these channels, in fact, already exist. But an explosion of new commerce channels and devices is creating something totally new environment where buyers and sellers will literally be able to conduct commerce anytime, anywhere and any way they like and for both buyers and sellers, this new environment provides more choice, more convenience, and more control over how they do business with one another, Integrating phenomenon as U-commerce" or universal, ubiquitous commerce. It is about the integration of more value-added information into each transaction, in ways that benefit both consumers and businesses.

U-commerce simply represents the still emerging destination of commerce initiated by E-commerce and propagated by M-commerce. Its purpose is to lay the groundwork for structuring future information systems and providing a discussion forum for trends in the field of Information system. U-commerce transforms the traditional commerce either geographic or electronic or mobile to a world of unique networks having a wide range of devices to invoke personalized services. An experimental set-up is chosen that examines how U-commerce fit into our traditional understanding of Information System.

Accordingly to **Watson et al., (2002)** U-commerce is defined as "the use of ubiquitous networks to support personalized and uninterrupted communications and transactions between a firm and its various stakeholders to provide a level of value over, above, and beyond traditional commerce"



U-COMMERCE PATH

In a ubiquitous computing environment, computing devices, applications, networks, and data will be fully integrated and merged. Almost any physical item can be embedded with computing power to establish a unique and verifiable identity, store a wealth of information, collect observations from the physical world, and sense changes in the environment. Ubiquitous computing has enabled a new paradigm of commerce which goes above and beyond any traditional commerce. This type of commerce is called "Ubiquitous/Universal Commerce", or simply "U-commerce", and is considered to be the ultimate form of commerce. U-commerce refers to the ability to interact and transact with anything and anyone, anytime and anywhere. Therefore, U-commerce is pervasive as it will become a part of everyday life and will be so prevalent that most people would not even notice its presence. U-commerce is going to be the next wave in commerce i.e., after E- commerce and M-commerce.

The advancement of new technologies such as radio frequency identification (RFID) and sensor networks has initiated a trend towards ubiquitous computing, which is also called "anytime, anywhere" computing. Technologies used in U-commerce such as RFID and sensor networks, have the ability to identify, track, and trace objects automatically. The use of such technologies has made it technically possible for service providers and merchants to deliver personalized products to their customers based on customers' preferences, and geographical locations.

U-commerce can provide a higher degree of personalization, which can provide additional benefits and value to customers. Despite the promising future of U-commerce and the tremendous benefits it can bring to customers, customers' privacy concerns appear to be the biggest obstacle and social issue. In order to enjoy the benefits of personalization in U-commerce, customers usually need to give up some of their personal information to the service providers or merchants. The advancement of technologies embedded and used in the U-commerce environment raises concerns of customers because their personal information not only can be constantly accessed and continuously tracked, but also can be easily disseminated and possibly used in ways unknown to them.

E- BANKING IN INDIA

Banking system always has an important role to play in every country's economy. It is vital for any nation as it provides for the needs of credit for all the sections of the society. India is not only the world's largest independent democracy but it is also an emerging economic giant. The growth potential of India is based on its strong banking institution. The infusion of information technology in banking sector has completely revolutionized how the banking sector operated. In order to survive in the new globalized world, banks had to opt for this new change.

The traditional method of banking was through branch banking. It was in 1991, that with economic reforms, the banking industry also witnessed the new wave of banking methods. It was Saraf Committee which was constituted by RBI in 1994 that recommended the use of Electronic Fund Transfer System (EFT), introduction of electronic clearing services and extension of Magnetic Ink Character Recognition (MICR) beyond metropolitan cities and branches. It was ICICI bank which became the pioneer of e-banking in India .It was the first bank to introduce online banking services in 1996. Its initiatives were followed by Citibank, IndusInd Bank and HDFC Bank who provided internet banking services in 1999.Various initiatives have been taken

by both the government and the Reserve Bank from time to time to smooth the expansion of e-banking in India. The Government of India enacted the IT Act, 2000 which provided legal recognition to electronic transactions and other means of electronic commerce. The important technological developments witnessed in the new age payment systems in India are:

- Arrival of card- based payments- debit card, credit card-
- Introduction of Electronic Clearing Service (ECS)
- Introduction of Electronic Funds Transfer/ Special (EFT)
- Real Time Gross Settlement (RTGS)
- Introduction of National Electronic Funds Transfer (NEFT)
- Introduction of Cheque Truncation System (CTS)

FEATURES OF E-BANKING

- 24x 7 banking hour service
- No geographical barrier
- Easy Electronic Fund transfer facility.
- Better efficiency in Customer relationship management.
- Making the Payments of bills like electricity, telephone bills, and mobile recharge.
- It can view of balance of accounts and statements.
- E-banking can bring doorstep services.
- Order mini statements.
- Mobile banking.
- SMS banking services

ISSUES IN ADOPTION OF E-BANKING

E- Banking today is a norm rather than an exception for the banks. But despite the fact that it offers number of benefits which make banking convenient and easy for customers, there are some issues that needs to be addressed .Some of which are stated below:

1.Security Risk : Security risk is the prominent challenge faced by the banks offering e-banking services .There are still many customers who refuses to opt for e-banking services because they still don't find e-banking or online banking secure. Online banking frauds like phishing, spamming, spy ware, internet theft etc. are still very much prevalent and are a thwart to e-banking expansion. These security problems need to be addressed to win over the confidence of the customers.

2. Privacy Risk: The risk of disclosing the private information of the customers with others. As all the information of the customers is available online, there is always a fear among the customers that their personal information may be shared by the banks with the marketing people.

3. Technical difficulties: As e-banking is all about the use of technology, any technical error can withholding the banking process. The problem of banking websites going down, or jamming problem due to lot of rush on the websites, blocking of the cards , forgetting log-in passwords all these are technical problems which a customer may face in using internet banking.

4. Customer Education: There are lots of users in India who still fear using e-banking services because they are unaware either about their benefits or are unaware about the mode of usage. It is a big challenge for the banks to make to slowly equip all the customers in using e-banking facilities. Though lot of people have shifted to use of ATMs and plastic cards, a lot needs to be done to make EFT and RTGS a popular banking mechanism among Indian users

PRIVACY AND SECURITY ISSUES

Security is simply the protection of interests. People want to protect their own money and bank their own exposure. The role of government is to maintain the integrity of and confidence in the whole system. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against system risk. This is serious role that cannot be left to the micro-economic interests of commercial organizations. The security of information may be one of the biggest concerns to the Internet users.

For electronic banking users who most likely connect to the Internet via dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated internet connections face the risk of someone from the internet gaining unauthorized access to their computer or network.

However, the e-banking system users still face the security risks with unauthorized access into their banking accounts. Moreover, the e-banking system users also are concerned about non-reputability which requires a reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transaction can be altered to change the apparent sender. Therefore, it is extremely important to build in non -reputability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.

PRIVACY AND SECURITY RISKS IN E-BANKING SERVICES

- Security and Privacy Threats in ATM
- Card and currency fraud
- Skimming
    i. External card skimming
    ii. Internal card skimming
    iii. Vestibule card skimming
- Card Trapping
- Currency Trapping
- Logical/data Attacks
- Malware and Hacking
- Physical Attacks

Security and Privacy threats in Internet Banking

- Phishing Attacks
- Spoofing

Security and Privacy threats in Mobile Banking

Almost similar techniques which are being used by fraudster in internet banking are being used in mobile banking for identity theft.

Security and Privacy threats in Credit cards

- Card Related Frauds
- Application Fraud
- Lost/ stolen cards
- Counterfeit cards
- Merchant Related Frauds

Internet Related Frauds

The most commonly used techniques in internet fraud are described below:

- Site cloning
- False merchant sites
- Credit card generators

Attacks on E-Banking

Hackers have many different ways that they can try to break into the system. The problems of the systems today are inherent within the setup of the communications and also within the computers itself. The current focus of security is on session-layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over un trusted channels, and a trustee code at both endpoints. It is really important to have a secure protocol because the trusted channels really don't exist in most of the environment. There are various types of attacks that e-banking can suffer. They include:

1. Social Engineering

One of the most common attacks does not involve knowledge of any type of computer system. Tricking consumer s into revealing sensitive information by posing as a system administrator or customer service representative is known as social engineering. Social engineers use surveillance and a consumer's limited knowledge of computer systems to their advantage by collecting information that would allow them to access private accounts.

2. Port Scanners

Attackers can use port scanners to ascertain entry points into a system and use various techniques to steal information. This type of software sends signals to a machine or router and records the message the machine responds with to ascertain information and entry point's .The main purpose of a port scanner is to gather information related to hardware and software that a system is running so that a plan of attack can be developed.

3. Packet Sniffers

The connection between a user's computer and the web server can be "sniffed" to gather an abundance of data concerning a user including credit card information and passwords. A packet sniffer is used to gather data that is passed through a network .It is very difficult to detect packet sniffers because their function is to capture network traffic as they do not manipulate the data stream. The use of a Secure Socket Layer connection is the best way to ensure that attackers utilizing packet sniffers cannot steal sensitive data.

4. Password Cracking

Password cracking can involve different types of vulnerabilities and decrypting techniques; however, the most popular form of password cracking is a brute force attempt. Brute force password attacks are used to crack an individual's username and password for a specific website by scanning thousands of common terms, words, activities, and names until a combination of them is granted access to a server.

5. Trojans

Trojan software is considered to be the most harmful in terms of E-Commerce security due to its ability to secretly connect and send confidential information. These programs are developed for the specific purpose of communicating without the chance of detection. Trojans can be used to filter data from many different clients, servers, and database systems. Trojans can be installed to monitor emails, instant messages, database communications, and a multitude of other services.

6. Denial of Service Attacks

Denial of service attacks are used to overload a server and render it useless. The server is asked repeatedly to perform tasks that require it to use a large amount of resources until it can no longer function properly. The attacker will install virus or Trojan software onto an abundance of user PC's and instructs them to perform the attack on a specific server. Denial of service attacks can be used by competitors to interrupt the service of another E-Commerce retailer or by attackers who want to bring down a web server for the purpose of disabling some type of security feature.

7. Server Bugs

Server bugs are often found and patched in a timely fashion that does not allow an attacker to utilize the threat against an E-Commerce web site. However, system administrators are often slow to implement the newest updates, thus allowing an attacker sufficient time to generate a threat. With the millions of web servers in use around the world, thousands often go without timely patches, leaving them vulnerable to an onslaught of server bugs and threats.

8. Super User Exploits

Super user exploits allow attackers to gain control of a system as if they were an administrator. They often use scripts to manipulate a database or a buffer overflow attack that cripples a system, much like a Denial of Service attack for the purpose of gaining control of the system. Users can create scripts that manipulate a browser into funneling information from sources, such as databases. Despite the various attacks on e-commerce, there are various defenses as noted below.

a) Education

Your system is only as secure as the people who use it. If a consumer chooses a weak password, or does not keep their password confidential, then an attacker can pose as that user. This is significant if the compromised password belongs to an administrator of the system. In this case, it here is likely physical security involved because the administrator client may not be exposed outside the firewall. Users need to use good judgment when giving out information, and be educated about possible phishing schemes and other social engineering attacks.

b) Personal firewalls

When connecting your computer to a network, it becomes vulnerable to attack. A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer. The intruder can also scan the hard drive to detect any stored passwords.

c) Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a protocol that encrypts data between the consumer's computer and the site's servers. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted. So that a hacker sniffing the network cannot read the contents. The SSL certificate is issued to the server by a certificate authority authorized by the government. When a request is made from the consumer's browser to the site's server using

d) Server firewalls

A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines. A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts.

e) Password policies

Ensure that password policies are enforced for consumer s and internal users.

f) Intrusion detection and audits of security logs

One of the cornerstones of an effective security strategy is to prevent attacks and to detect potential attackers. This helps understand the nature of the system's traffic, or as a starting point for litigation against the attackers. Suppose that you have implemented a password policy: If a consumer makes 6 failed logs on attempts, then his account is locked out. In this scenario, the company sends an email to the customer, informing them that his account is locked. This event should also be logged in the system, either by sending an email to the administrator, writing the event to a security log, or both.

Security and Privacy Regulatory Environment

The part primarily focuses on Reserve Bank of India‘s guidelines issued from to commercial banks with respect to security and privacy of Internet Banking, ATMs, Mobile Banking, and Credit Cards etc.

Security and Privacy regulatory environment

Internet Banking is a popular and convenient method of doing online banking transactions but there is no dedicated Internet banking laws in India. However, Reserve Bank of India (RBI) has been consistently making efforts to bring more make internet banking transactions more and more secure. During the year 2010, Reserve Bank of India set up a Working Group under the Chairmanship of S.R Mittal to address the Regulatory and Supervisory concerns in internet banking focusing on

i) Legal and regulatory issues,
ii) Security and technology issues
iii) Supervisory issues

CONCLUSION

In this paper it has been concluded that U-Commerce is a continuously emerging field of wireless communication in the present age and one of the non-negligible technology in the market place. U-Commerce enables users to connect the whole world anytime and from anywhere. The major findings are:

- U-Commerce technology was perceived to be very useful for location-independent tasks.
- None of the technology either wireless or wired, turned out to be superior in terms of perceptions of ease of use. Through U-Commerce we can achieve high performance of non-location dependent tasks.

In short, we say that U-Commerce is the creation of a marketplace and a landmark of wireless technology, which reaches individuals where they can want to use, with the networks technology.

The internet has grown exponentially, enhances the interaction between two businesses as well as between individuals and business. As a result of the growth of the internet, electronic commerce has immerged and offers tremendous market potential for today's business. One industry that has benefited from this new communication channel is the banking industry.

Electronic banking (e-banking) is offering its customers with a wide range of services. Customers are now able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions. E-banking is offered by many banking institutions due to pressure from competitions. Today, it is believed that people make the difference to information technology and security development and that training on the ethical, legal and security aspects of information technology usage should be ongoing at all levels within organizations

The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard. it have indicated that the common problem affecting information security and privacy of customers is e-services provider's lack of security control which allows damaging privacy losses. Apart from that, another problem is the subsequent misuse of consumers' confidential information, as in identity theft. These may affect customer's confidence toward online business transaction in a variety of privacy risk assessments by consumers. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the consumer to be vigilant when doing business online.

Reference:

1. James Gleick, **"Connected: Life in the Wireless Age,"** New York Times Magazine, April 22, 2001

2. Gupta V, (2002). **"Overview of E-banking", E-banking:** A Global Perspective Bankers

3. Kahikara, M., and Sorensen, C. **Post Modern Professional Work and Mobile Technology** 25th (IRIS25), August 2002, Denmark

4. Junglas, I.A. **U-Commerce: An Experimental Investigation of Ubiquity and Uniqueness,** University of Georgia, Dissertation, Athens, 2003.

5. Rao N K, **"Indian Banking system:** The Forward Banker, February 2005.

6. Brar, A., Kay, J.: **Privacy and security in ubiquitous personalized applications**, available ethttp://www.cs.usyd.edu.au/ judy/ Homec /Pubs/2005_Ajay_Brar_PEP.pdf, Accessed: May 2009

7. Dr. Paul Cesarini, **"The Fall and Rise of Information Appliances",** Journal of Literacy and Technology Volume 10, Number 3: November 2009