**Global Journal of Multidisciplinary Studies** Available online at www.gjms.co.in
Volume 2, Issue2, January 2014
ISSN: - 2348-0459

# AN ANALYSIS OF E – COMMERCE AND ITS EFFECT ON CURRENT SCENARIO

**DINKER JHA** [1]
Belan Bazar, Bangali Tola, Braham Niwas, Dist. – Munger 811201 (Bihar)
**DEVDUTTA INDORIA** [2]
Nice college of commerce, circuit house road, balangir,

ABSTRACT

Technology innovations in the banking sector, have been shown to increase productivity of this industry around the world. Using online banking or Internet banking is often the most convenient way to transact all our banking business. When we have online access to our financial information we can pay bills, move money from one account to another, and simply take care of all our business without walking into local bank branch. Use of internet banking is becoming common because no one wants to take the time to stop at the bank to get things done. When we use Internet banking, everything we need can be done from the comfort of our own home or office. The great thing is we don't have to change banks to take advantage of the Internet bank capabilities. Most banks offer online banking, giving us complete access to our bank accounts, our loans, and even to bill payments. This means we can log on, move money around, pay bills including loans and mortgages, and that is all. There is no need to stop at the bank to move money from savings to checking. We might even be able to order cheques online. If we really want to save time, we can even get our bank statements through Internet bank, doing away with all of that paper that stacks up in filing cabinet.

**Key word: -** Technology, banks, change

## INTRODUCTION

The advent of e-commerce through the Internet1 and its' continued growth has spawned many changes in the way business is being conducted. Like that of the industrial revolution, e-commerce promises to accelerate the rate of growth and development of the world economy. The Forrester Research by far showed the largest estimates of ecommerce in the year 2000-global business-to-business (B2B) e-commerce alone was estimated to be US$604 billion UNCTAD (2001).

Now, a question arises is online banking safe? Yes. Banking online is safe and convenient way to manage our money and there is no reason why the Internet cannot be use with confidence. However, we should not relax our guard when online. We should be more suspicious of an unsolicited email than of a stranger knocking at the front door, because it is harder of us to ask email sender to prove the real identity they claim.

Information security is now a major issue facing today's electronic society. As the information highway transcends boarders. Locked doors are not longer sufficient to protect one of the corporation's most valuable assets -information. As business-to-business (B2B) or business-to consumer (B2C) e-commerce takes off and more and more businesses shift their primary service onto the Internet, the need for tight and controlled security measures is essential for survival.

These days Internet security is at the forefront of online baking priorities. Customers demand access to financial information and personal and business accounts 24 hours a day, 7 days a week. As we move into the electronic world how can we recognize and trust people when we can't see them, hear them or even receive their signature? How do we keep our business transactions secret without sealed envelopes or private telephone calls? How do we know the intended person received the message intact and has agreed to the contract?

Any downtime caused by information security branches has an immediate and significant impact on customer satisfaction and revenues. Financial institutions must employ a variety of best-of-breed solutions to help prevent unauthorized access to the network to ensure the

full confidentiality and reliability of all e-commerce transactions.

Consumers and businesses engaging in Internet-based commerce are looking to reproduce some of the safeguards they rely on for traditional face-to-face transactions when negotiating contracts or conducting exchanges.

To accomplish this task successfully, three key points need to be established.

- The first is a strong assurance of the identities of the transacting parties. In the physical world, identify is established through presentation of credentials.
- The second is the ability to ensure that the transactions are both confidential as well as unchanged by the medium.
- The third requirement is a way to record the terms of agreements or contracts to allow mutual and third party audit and, if necessary, legal action.

Most of today's Internet transactions fail to meet these three requirements.

**AN ILLUSTRATION OF ONLINE FRAUD:**

When a hacker or even internal authorized user targets a website, it can be seriously detrimental to the financial institute or a bank and of course to the businesses of the customers. For example, a hacker has decided to manipulate the banking transaction. He systematically attacks the users who are online at one of the larger online banks. By steadily guessing passwords in such a way as to hide that he is doing so (to defeat security measures designed to detect this), the hacker is able to slowly crack a few dozen user accounts. These accounts are then probed for useful information such as trading patterns, portfolio size, and portfolio makeup. Once the hacker has established what the usernames and passwords are, he is ready to strike. He might change or transfer the account credits to another account or even popular attacks like 'salami' fraud to round-off zeros in truncating numbers. When actual account holders discover the discrepancies in their accounts, they will be told by the bank that the transaction was carried with the password issued to the user which is the only proof. In such case the poor account holder may have suffered a financial loss and a loss of privacy.[4]

Now in order to extend the trust of the customers in online banking system, the banking applications shall have the following features :

- Authentication

Validates the identity of each party or user in the transaction.

- Authorization

Allows rules to dictate who uses what resources and under what conditions.

- Confidentiality

Protects confidentiality of sensitive information, while stored or in transit.

- Integrity

Ensures the messages have not been altered or terflpered while in transit or

stored in online databases.

- Non-repudiation

Prevents any party or user from denying a tran after the fact that digital

signatures are associate the transaction.

- Audit controls

Provides audit trails and recourse for all users.

There are some myths about e-security perceived by the application providers that no further security is required on the application if firewall, Secured Socket Layer (SSL),File Permission server, etc are there.

Firewalls protect a system from a different class of risks by preventing access to non-public services and prevent malicious network traffic from reaching the server. Firewall approach achieves security by isolating a specific

segment of internet topology (further local network) from the rest of the internet and controlling all the traffic that comes to and leaves the local network.

File permissions may prevent abuses of rights when different user levels are involved but is will not do so between two users with the same level.

SSL provides server (and sometimes client) authentically and communication privacy, but otherwise it is blind content of the traffic.

Some application developers are of the opinion that security can be embedded subsequently from a third. This type of third party add-ons are never tested for interoperability, scalability and security aspects of the party product itself. The security needs to be built in application from the beginning. It is not something to apply at the end.[2]

**PUBLIC KEY INFRASTRUCTURE (PKI) :**

Internet banking communications can be linked to an electronic equivalent of signing a cheque and sealing envelope. The act of signing a cheque is evidence of authenticity and non-repudiation and the act of sealing the envelope assures confidentiality and integrity.

Symmetric cryptography ensures confidentiality by encrypting a message using a secret key in association with an algorithm. This produces a 'scrambled' version of the message that the recipient alone can decrypt using the same shared secret key. The key used must be kept secret by both the parties and distributed to each other in a secured manner. The problem with this type or cryptography is securely managing and distributing the secret key. As the proof of non-repudiation cannot be assured as both parties have access to the secret key.

Public key cryptography (or asymmetric cryptography) solves this problem by replacing the secret key with a pair of keys; one private and one public, both mathematically linked to one another, information is encrypted with the public key, which can only be decrypted with the corresponding private key from the key pair, providing proof of confidentiality. In this system, the public keys of all users can be published in open directories, facilitating communication between all parties.[1]

The private key is shared, only the public key is made public. Public key cryptography can also be used to create and verify 'digital signatures'. These can be appended to message to provide proof of authentication, integrity and non-repudiation. Hence, PKI technology offers the best means to fulfill requirements as needed by secured online transactions.

However, public key cryptography on its own is not enough if we are to truly recreate the conditions for traditional paper based transactions in an electronic world. We also need.

- Security policies to define the rules under which the cryptography systems should operate and
- Secured storage and management of the keys.

PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the following 4 principal security functions for commercial transactions like Internet banking.

1. Confidentiality
2. Integrity
3. Authentication
4. Non-repudiation

Lack of security is often cited as a major barrier to the growth of e-commerce and internet banking, which can only be built on the confidence that comes from knowing that all transactions are protected by these core functions. Like any new business-critical technology, the evaluation and implementation of a PKI solution is a challenging and intricate process, which requires a great deal of planning, management and clear guidance.

Today, use of PKI has reduced that need of paper sharing as it is a secured and transparent process. As digital signature cannot he repudiated, digital transactions get legal foundations too.

**CONCLUSION**

It is clear based on the rational expectation of buyers and sellers that electronic commerce will continue to expand

in the region. With this growth predicted the import and export of products, both traditional and digital, are likely to increase. In the import market increase imports of traditional goods and services will lead to increase tax and tariff revenues, while increase imports of digitised goods will not. Some revenues will be lost from the displacement and/or reducing market share of uncompetitive firms located in the region. The magnitude of revenue changes will depend on changing volumes of imports and exports, which in turn will depend on elasticity in both markets.

**REFERENCES**

1. Andal, F. D, (1997), 'State and Local Taxation of Electronic Commerce: Read My Email,

2. no new taxes', April. Harvard Law School International Tax Program and The Society for Law and Tax policy.

3. Caribbean Organisation of Tax Administrators General Assembly, (2000), "The Impact of the Growth of the Internet and Electronic Commerce on Tax Administration', Prepared by the United States Internal Revenue Service.

4. Case, Wendy and Charles Ramires, (2000), 'Despite the ruling it will be hard to stop free music exchange', The Detroit News, Friday, July 28 2000.

5. Chaitoo, Ramesh, (2000), 'Electronic Commerce and CARICOM Economies: Strategic Eastern Caribbean Central Bank, (1999), 'The Tax structures of Barbados, Jamaica, Guyana and Trinidad and Tobago.'