Distributed Securities Against Eavesdropper in Electronic Funds Transfer

Chetan Raikwar*
Jitendra Sheetlani**

Abstract

Many people have speculated that cash and checks will eventually go the way of the dinosaur or the passenger pigeon; that is, at some point, they will cease to exist in the market, having been replaced by new emerging, electronic payment methods. Generally the banking laws, regulations and supervision were designed primarily to address the fundamental principle relating to safe and sound business practices by financial institutions. For many consumers, electronic banking means 24-hour access to cash through an automated teller machine (ATM) or Direct Deposit of paychecks into checking or savings accounts. But electronic banking now involves many different types of transactions.

Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. Electronic funds transfers are based on technology that by its nature is designed to extend the geographical reach of banks and customers. This kind of a market expansion extend beyond borders, therefore there will be problems which banks will try to avoid like regulation and supervision.

Electronic Funds Transfer (EFT) provides for electronic payments and collections. In this paper we discuss about new electronic payment methods and different securities level of distributed database. We also Discuss the distributed securities of Electronic funds Transfer. The aim of this article is to briefly examine and explain the issues of electronic funds transfers, security and privacy of transactions pertaining to internet payments. This paper introduces electronics funds transfer, discusses some of their basic properties of EFT and outlines their general role in securing software applications on the EFT. In addition, the architecture of a EFT is described.

Keywords: - *Electronic Funds Transfer, Distributed Database system, securities level, data transaction.*

Introduction

Electronic fund transfer has been around and accepted by customer in the form of ATM's and telephonic transactions; however, Internet banking has transformed electronic banking and serves as a remote delivery channel. **Electronic fund transfer system** (**EFTS**) refers to a variety of systems and technologies for transferring funds (money) electronically rather than by check. It consists of a group of technologies that allow financial transactions to be carried out electronically. Electronic funds transfers are recognised and accepted globally.

The history of EFT originated from the common funds transfer of the past. Since the 19th century, and with the help of telegraphs, funds transfers were an usual thing in commercial transactions. Finally, it migrated itself to computers and become the electronics money transfers of today.

Security concerns impose a severe constraint on a vast array of products and services that can be offered within the context of the EFT. The security of EFT systems is of important public concern. Customer want a payment mechanism which is safe, to be able to make and receive a payment and get assured that no-one can divert such payment or impersonate them in order to steal their funds. In this article it is to briefly examine and explain the issues of electronic funds transfers, security and privacy of transactions pertaining to Internet payments.

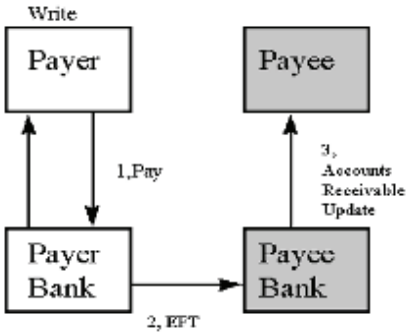
What Is EFT or Electronic Funds Transfer

Electronic funds transfer or EFT is the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions, through computer-based systems. It is provides for the electronic payment and collection of money and information. EFT is safe,

*Assistant Professor, Pioneer Institute of Professional Studies, Indore
**Assistant Professor, LNCT, Indore

secure, efficient, and less expensive than paper check payments and collections.

An electronic funds transfer is a system for transferring money from one bank to another without using paper money. Its use has become widespread with the arrival of personal computers, cheap networks, improved cryptography and the Internet. Since it is affected by financial fraud, the electronic funds transfer act was implemented. This federal law protects the consumer in case a problem arises at the moment of the transaction.



In above Figure, the payer receives a bill/invoice from his bank, (assuming electronic bill presentment allows for capture of the payee's bills by the payer's bank), issues an Electronic Check, and sends it to his bank. The payer's bank, in turn, transfers funds to the payee's account at the payee's bank.

The mechanism of EFT is built on a complex network infrastructure connecting to another network infrastructure through the Internet. If the network infrastructure security itself is lacking then data via electronic transaction may be in danger. With EFT, there must be a proper infrastructure to manage the identity of users.

Advantage and Disadvantage of EFT

Electronic Funds Transfer (EFT) is a system of transferring money from one bank account directly to another without any paper money changing hands. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments. The benefits of EFT include reduced administrative costs, increased efficiency, simplified bookkeeping, and greater security. There are following advantages and disadvantages of EFT.

Advantages of EFT

- The main advantage of EFT is Time. Since all the transactions done automatically and electrically.
- The money (wages) can be transferred to the workers' bank account at any time and there is no need for the manager to leave the comfort of his office to perform this transaction.
- No delay connected with paperwork.
- No need for cheques or cash. All the transaction done by electrically.

Disadvantages of EFT:

- **Required Special Equipments** – Electronic conversion requires special equipments. So the cost of investment may increase.
- **Uses Computer Networks** – Electronic method means computer networks are used for transferring data. This also means, the problems occurring on computer networks can affect the transactions of electrically.
- **Unauthorized Transactions** – Unauthorized transactions can occur in EFT too. Thus, it is always advised to keep record of your physical cheques. You can also check your bank statements for any unauthorized transactions.

As you can see EFT has many advantages and disadvantages. However, the advantages supersede the limitations to make this one of the chosen method of paying somebody.

EFT's Related Technologies

EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Cash card and point-of-sale (POS) transactions. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments. One of the most common EFT's technologies is

- Direct Deposit. It is used by employers for depositing their employees' salary in a bank account. Other kind of EFT is the automatic charge to your check or savings account. For example, when you are paying a mortgage, the bank will discharge the monthly payment from a pre-accorded bank account. The benefit is that you won't have to go to the bank to do it. It's automatic.
- Another kind of EFT is a cash card. With this type of card you can spend a prepaid amount of money until the balance is zero. So, if you wish to make a gift certificate without tying up your beneficiary with one store, you can buy a cash card from your

favorite bank.

- ATM's are also used for EFT's. Since an automatic teller machine is much cheaper than a group of bank tellers, it has helped to bring costs down and beneficiate the costumer.
- Points of sale (also known as POS) are also part of this group. Those little blue or dark blue machines in which you pass your card are doing an electronic fund transfer from your account to the retail account. Imagine how the world without them was. Slow, wasn't it?

Security Issues

Security means the protection of the integrity of electronic funds transfer (EFT) systems and their information from illegal or unauthorized access and use. Without the proper security implementation, our information is not safe. There are numerous threats aimed at destroying critical infrastructure, stealing important data, identity and intercepting communications and destroying trust and confidence in the use of Internet for critical transactions.

Within the context of any Electronic funs transfer, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

Then, not only protects data from theft or alteration, but can also be used for user authentication.

Eft Security Technique (Encryption)

The major categories of threats to EFT security are summarized as follows. In theory, nearly all of these can be minimized by the application of good management practices. The three lines of defense against breaches of EFT security are administrative procedures, physical protection, and technical/ electronic safeguards.

Internal Threats (Within the Institution)

- **System failure:** Failure of computer programs
- Failure of hardware components
- Loss of data from system malfunction
- Deterioration of storage media
- Failure of communication links
- Failure of power, destruction of facilities
- Deterioration of storage media Employees
- greed. malice, Ineptitude accidents, disgruntlement, challenge
- Trojan horse (unauthorized procedures hidden within programs)
- Bogus transactions
- Unauthorized copying of data or programs
- Modification of data
- Unauthorized sale of data
- Destruction

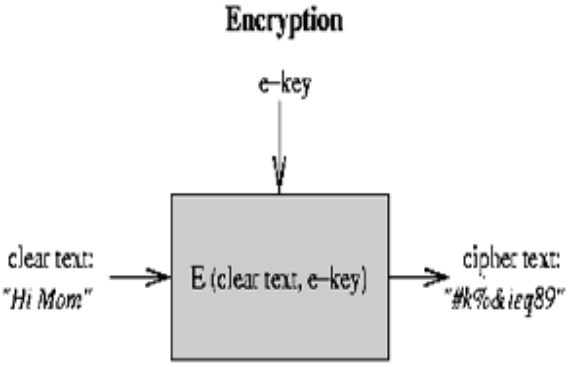
External threats to system

- Natural disaster: fire, flood, ice and snow, earthquake, etc.:
- Direct damage
- Lack of maintenance
- Overload at terminals
- Inaccessibility
- Human
- criminals, terrorists, political (and religious,
- economic, racial) activists, “buff s,” Inept
- customers
- Physical damage (Including vandalism) or
- destruction
- Destruct Ion of data
- Modification of data
- Theft of data
- Fake transactions
- Impersonation of computer
- Forged access devices
- Unauthorized use of access devices

The best protection for data in transmission and in storage is probably encryption. One form uses encoding in which the coding and decoding procedures are public but the actual encryption keys used are secret and tightly controlled. The National Bureau of Standards has developed a national encryption standard called the Digital Encryption Standard

(DES). DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS).

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is **encrypted** information (in cryptography, referred to as ciphertext). In many contexts, the word **encryption** also implicitly refers to the reverse process, **decryption** (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted)



Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. We can have two kinds of encryption:

1. **Symmetric Key Encryption:** There is a single key which is shared between the two users and the same key is used for encrypting and decrypting the message.
2. **Public Key Encryption:** There are two keys with each user : a public key and a private key. The public key of a user is known to all but the private key is not known to anyone except the owner of the key. If a user encrypts a message in his private key then it can be decrypted by anyone by using the sender's public key. To send a message securely, we encrypt the message in the public key of the receiver which can only be decrypted by the user with his private key.

Symmetric key encryption is much faster and efficient in terms of performance. But it does not give us Non-repudiation. And there is a problem of how do the two sides agree on the key to be used assuming that the channel is insecure (others may snoop on our packet). In symmetric key exchange, we need some amount of public key encryption for authentication. However, in public key encryption, we can send the public key in plain text and so key exchange is trivial. But this does not authenticate anybody. So along with the public key, there needs to be a certificate. Hence we would need a public key infrastructure to distribute such certificates in the world.

Security solutions

Security means the protection of the integrity of EFT systems and their information from illegal or unauthorized access and use. Although the loss per theft appears to be greater than for paper-based payment systems, there is no real evidence that EFT systems to date have resulted in a higher than average crime rate. The security of EFT systems is an important public concern and potentially a major policy issue. In comparison with other payment systems, EFT appears to have some additional vulnerability. There are following security solutions for secure EFT.

1. The use of Encryption technologies such as Digital signature and Digital certificates.
2. 24/7 monitoring should be put in place that will alert the relevant people to take the necessary action.
3. Security Awareness is important in today's digital world.
    - Use a secure browser.
    - Use a credit card.
    - Never store your credit card number on the site, if possible.
    - Never store your credit card and password info in your computer.
    - Always change your username and password regularly.
    - Shop at trusted companies.

Conclusion

Electronic Funds Transfer (EFT) provides for electronic payments and collections. EFT is efficient and less expensive than paper check payments and collections. The benefits of EFT include reduced administrative costs, increased efficiency, simplified bookkeeping, and greater security. EFT needs security of data for safe and secure transaction. Without the

proper security implementation, our information is not safe. There is an urgent need for the establishment of the Computer Security Response Team, which must protect and secure information. High degree of security and privacy is of utmost importance to the future regulation, protection and use of Internet banking because of the challenges it poses on the payment system.

References

1. Bamford, J. Body of Secrets : Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century. New York: Doubleday, 2001.
2. Bauer, F.L. Decrypted Secrets: Methods and Maxims of Cryptology, 2nd ed. New York: Springer Verlag, 2002. Denning, D.E. Cryptography and Data Security. Reading (MA)
3. Leonard Krauss and Aileen MacGahan, Computer Fraud and Coun term easures(Englewood Cliffs, N. J.: Prentice Hall, 1979).
4. Edward H. Coughran, Crime by Computer (University of California San Diego computer Center: 1976).
5. S240, Federal Computer Systems Protection Act, January 1979.
6. Telecomrnunications Systems to Unauthorized Use (1977).
7. Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity March 1982.