E-Cash For Safer Online Transactions

Abstract

Today technology has revolutionized all the fields including banking. Driven by the internet phenomenon, banks have introduced online banking. It allows the user to perform banking transactions online. Due to the enormous development of e-commerce we are able to purchase anything online. But paying online is still a challenge. Currently debit cards and credit cards are used to pay online which incur high transaction cost and it's not secure. To overcome this money has to be digitized. E-cash allows transferring digital money through a secured channel. In this paper we will review some cryptographic algorithms which ensure the security of digital money. To shop online e-coins can be used to make payments. E-coin contains the value of money, serial number, issuing bank and date of expiry. It is encrypted and digitally signed by the bank using blind signatures. Serial number is unique which detects double spending. E-cash offers both secure online and offline payments. Customers can request e-coin from the bank by specifying the denomination. Bank sends the encrypted digitally signed e-coin to the customer. It can be paid to the merchant and it can be deposited in merchant's e-cash account to get real money. Customer need to open digital account with the bank to utilize digital money.

1 Introduction

Internet technology has become an important aspect of our day today life. A organization which misses the bus of IT, is left behind the race. Due to the development of e-commerce there is a large demand for digitizing money. E-cash is a payment system which is designed in such a way that it allows making secured online transactions. It involves digitizing money, e-cash crosses into the domain of politics, economics,law,history etc, as well as attracting the attention of numerous technology and communication companies. Enhanced security for this application can be achieved by using complex cryptographic algorithms, such as threshold blind signatures and digital signatures.

Archenaa Jothi Msc Software Engineering in PSG College Of Technology from Anna University
Email:archenaa.barani@gmail.com

1.1 What Is E-Cash?

It is an application which allows transferring digital money – e-coins through a secured channel. The user doesn't need to go straightly and wait for hours to fill all the applications. This would be a tedious process and time consuming. In addition, micro payment system like E-cash provides a service which allows users to perform secure electronic financial transactions with a full suite of payment solutions for the Internet. It allows the user to request e-coins from the bank and make the payment through secured network.

2 Technical Methods Used In The System

In electronic commerce, the challenges of payment transactions were

initially underestimated. Business via the internet and mobile telephony has so

far been dominated by the methods of payment customary in traditional

business. However, in light of advances in e-commerce, traditional business

models are increasingly coming up against their limits.

Electronic payment systems are becoming more attractive for large financial

institutions. The systems already used in traditional offline business and which

have been adapted to meet the new demands of e-business have very good prospects

of convincing online customers.

2.1 Challenges Faced By Micro Payment System

The major issues are:

- Security is an issue in micro payment systems like E-cash.
- Secure, user friendly and low-priced innovative payment solutions are urgently required to boost internationally oriented e-commerce.
- Security is the key criterion for electronic payment systems. Critical issues are authentication, authorisation, privacy, integrity and data corruption.
- **Authentication** is another issue in an Internet banking system. Transactions on the Internet or any other telecommunication network must be secure to achieve a high level of public confidence.

2.2 Electronic Cash Issues

- Must be anonymous, just like regular currency
- Safeguards must be in place to prevent counterfeiting
- Must be independent and freely transferable regardless of nationality or storage mechanism
- Atomicity
  - Money is not lost or created during a transfer
  - Money and good are exchanged atomically
- Non-repudiation
  - No party can deny its role in the transaction
  - Must Detect Double Spending

2.3 Providing E-Cash Security

- Complex cryptographic algorithms prevent double spending
- Anonymity is preserved unless double spending is attempted
- Serial numbers can allow tracing to prevent money laundering.
- Threshold blind signatures are used.

3 E-Cash Implementation

3.1 E-Cash Concept

1. Consumer buys e-cash from Bank
2. Bank sends e-cash bits to consumer (after charging that amount plus fee)
3. Consumer sends e-cash to merchant
4. Merchant checks with Bank that e-cash is valid (check for forgery or fraud)
5. Bank verifies that e-cash is valid
6. Parties complete transaction: e.g., merchant present e-cash to issuing back for deposit once goods or services are delivered.

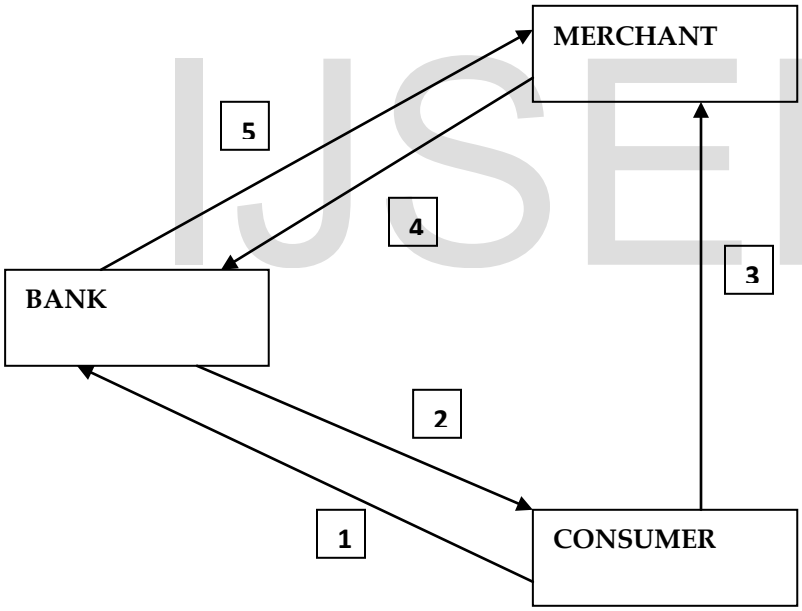

Fig-1 E-Cash Concept

3.2 Blind Signatures And Its Implementation

3.2.1 Blind Signatures

Blind signature scheme is a protocol that allows the provider to obtain a valid signature for a message **m** from the

signer without him seeing the message and its signature.

- If the signer sees message ***m*** and its signature later, he can verify that the signature is genuine, but he is unable to link the message-signature pair to the particular instance of the signing protocol which has led to this pair.

3.2.2 Need For Blind Signatures

- To sign the e-coin message by the bank without knowing the content.
- To provide anonymity with authentication.

3.2.3 RSA Based Blind Signature Scheme

1. The bank has the RSA private key d and the corresponding public key (n, e).
2. You want the bank to sign m, but you don't want the bank to see m.
3. Choose a blinding factor B at random, a non-zero resudue mod n.
4. Compute s = m · Be(mod n).
5. Ask the bank to sign s.
6. The bank computes t = sd(mod n) and sends t to you.
7. You then compute r = t · B−1(mod n).

3.3 Cut And Choose Algorithm

1. Prepare *n* copies of the messages and *n* different keys, and send them to the bank .
2. The bank requests the keys for and opens *n* - 1 of them, and verifies them. It then signs the remaining one.
3. The bank sends back the signed message, which can then be decrypted and spent

3.4 Anonymous E-Cash Principle


Unblinded, Unsigned


Blinded, Unsigned


Blinded, Signed

Unblinded,Signed

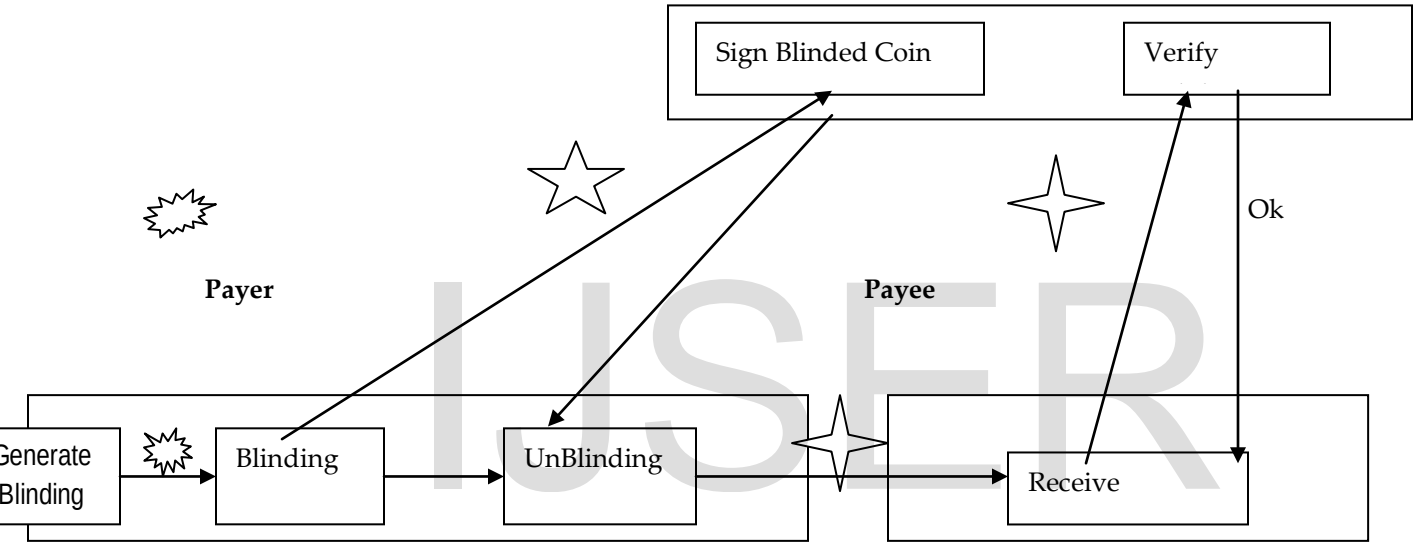

Fig-2 Anonymous E-Cash Using Blind Signatures

Summary

In the present situation where the technology is the buzzword and has revolutionized the way we work and live, we would be the losers if we do not keep up with the changing world. Moreover, it makes a world of difference and a whole of sense to break-up from the age old work culture and embrace the effective, cost, and time saving ways of looking and working at things.

This is precisely where the Electronic Cash System fit into place. E-CASH crosses into the domain of politics, economics, law, history etc, as well as attracting the attention of numerous technology and communication companies.

E-Cash allows users to perform secure electronic financial transactions with a full suite of payment solutions for the Internet including registering for digital cash account and users can also deposit to and withdraw from their E-Cash account and also make payments through E-coins. Enhanced security for this application is provided by using complex cryptographic algorithms and blind signatures.

These customized programs are effective and easy to handle with good help facilities and it is highly scalable, viable and user friendly. Also the system is done with an insight vision of considering necessary modifications that may require in the future.

Using such a system helps the users in minimizing the time consumed in fulfilling the day-to-day functionality's and cutting down the expenses incurred on the same.

Ref Literature Cited

1. Jesse Liberty, O'Reilly, 2005, *Programming C#*.
2. Steve Teilhet, Jay Hilyard, *C# Cook Book* .
3. Michael J.Corey, Michael Abbey, Ian Abramson, *Oracle9i A Beginner's Guide.*
4. Ben Chang, Mark Scardina, Stefan Kirtizov *Oracle9i XML Handbook*
5. Benoit Marchal, Que Publishing, Inc,2001, *XML by Example*.
6. Peter Thorsteinson, G.Gnana Arun Ganesh, Prentice Hall,2003, *.Net Security and Cryptography.*
7. http://www.triton.towson.edu/~mzimand/acrypto/N10-Protocols.pdf
8. http://www.csd.uoc.gr/~manifava/projects/IS-L2a-23-project3-eCash.pdf