Comparison of Current On-line Payment Technologies

Master thesis performed in division of Information Theory

by

Ravi Kumar Mandadi
LiTH-ISY-EX--06/3847 --SE

Comparison of Current On-line Payment Technologies

Master thesis in division of Information Theory,
Dept of Electrical Engineering,
at Linköping Institute of Technology.

by

Ravi Kumar Mandadi

LiTH-ISY-EX--06/3847--SE

Supervisor and Examiner: Prof. Viiveke Fåk
Abstract

The purpose of this thesis work was to make a survey of current on-line payment technologies and find out which are they and how do they work? Compare and analyze them from a security point of view, as well as a usability point of view. What is good? What is bad? What is lacking?

To achieve this purpose, an overview of the current on-line payment technologies was acquired through academic books and papers, Internet sites, magazines. Basic cryptographic and security related techniques were studied for the security analysis of current on-line payment systems. In this work, various current on-line payment systems were classified into two groups [Macro and Micro on-line payment systems]. This classification was based on the mode of on-line payment transactions. To analyze these on-line payment systems, a set of payment system requirements were formed [Security Issues, Usability Issues, Anonymity, Scalability etc].

Under the category of Macro payment system, Credit Card payment system, Debit Card payment system, Stored Value Card payment system, Electronic Check payment system, Electronic Cash payment system, Electronic account transfer payment system and mobile payment system transactions were examined. Under the category of Micro payment system, Hash Chain based Payment System, Hash Collisions and Hash sequences based Payment Systems, Shared Secrete Keys based Payment Systems and Probability based payment systems were examined.

Based on the requirements of payment system, these on-line payment systems were analyzed and compared. In the analysis phase, the advantages and drawbacks of these payment systems were figured out. It was found from the study that the credit card based payment systems are the most widely used means of conducting on-line payments. It is evident that credit card based payment systems satisfy stakeholder requirements the best, as they offer more flexible payment options, having a large user-base, benefit from familiarity and simplicity of use and also allow international payments. The other on-line payment systems lack this flexibility. It can also be extracted from the study that users want more simplified, convenient and secure on-line payment systems. Thus the futuristic on-line payment systems will have all secure payment options into one system.

Keywords

On-line payments, Macro Payments, Micro Payments, Comparison of Payments, Electronic Cash, Electronic Check, Electronic Account Transfer, Mobile Payment systems.
Abstract

The purpose of this thesis work was to make a survey of current on-line payment technologies and find out which are they and how do they work? Compare and analyze them from a security point of view, as well as a usability point of view. What is good? What is bad? What is lacking?

To achieve this purpose, an overview of the current on-line payment technologies was acquired through academic books and papers, Internet sites, magazines. Basic cryptographic and security related techniques were studied for the security analysis of current on-line payment systems.

In this work, various current on-line payment systems were classified into two groups [Macro and Micro on-line payment systems]. This classification was based on the mode of on-line payment transactions. To analyze these on-line payment systems, a set of payment system requirements were formed [Security Issues, Usability Issues, Anonymity, Scalability etc].

Under the category of Macro payment system, Credit Card payment system, Debit Card payment system, Stored Value Card payment system, Electronic Check payment system, Electronic Cash payment system, Electronic account transfer payment system and mobile payment system transactions were examined.

Under the category of Micro payment system, Hash Chain based Payment System, Hash Collisions and Hash sequences based Payment Systems, Shared Secrete Keys based Payment Systems and Probability based payment systems were examined.

Based on the requirements of payment system, these on-line payment systems were analyzed and compared. In the analysis phase, the advantages and drawbacks of these payment systems were figured out.

It was found from the study that the credit card based payment systems are the most widely used means of conducting on-line payments. It is evident that credit card based payment systems satisfy stakeholder requirements the best, as they offer more flexible payment options, having a large user-base, benefit from familiarity and simplicity of use and also allow international payments. The other on-line payment systems lack this flexibility.

It can also be extracted from the study that users want more simplified, convenient and secure on-line payment systems. Thus the futuristic on-line payment systems will have all secure payment options into one system.
Acknowledgments

This thesis work would not have been possible without the help and guidance of a lot people. It is now time to thank all of those, who have contributed to this master thesis work.

It seems appropriate to start with the person, who suggested me this thesis work, my examiner and supervisor Prof. Viiveke Fåk. She gave me an opportunity to work on this master thesis work under her esteemed guidance. She supported me with excellent suggestions and comments whenever I needed them, no matter whether she had time to deal with my questions or not. I was lucky to get the best possible supervisor. I am grateful to her.

I am grateful to Mr. Per Lindström, Director of Studies in Computing Science Department at Umeå University, for giving me the opportunity to conduct my master thesis at Linköping University and supporting me to complete my master studies at Umeå university.

I am thankful to my thesis opponent David Akhvlediani for his valuable suggestions, which helped me to improve the quality of work.

Reading a long thesis can hardly be fun. So a big thanks to Kameswar Rao Vaddina for helping me to improve the thesis report by proof reading and correcting grammar, even if it was not his main field of interest.

I thank God for my existence, encouragement and leading. I am grateful to my parents, family members and colleagues for understanding my priorities during this period of time.

I would like to thank my Christian friends, Mike Fahl and Ravi Pasupuleti for their prayer and moral support.

I would like to thank Purushotham and Praveen Nalli for all help, nice coffee breaks and interesting lunch conversations during thesis work.
Table of Contents

1. Introduction to On-line Payment Technologies ................................................................. 1
   1.1. What is On-line Payment? ......................................................................................... 1
   1.2. Motivation for On-line Payments ............................................................................ 1
   1.3. Security Concerns of On-line payments ................................................................. 2
      1.3.1. Double Spending Electronic Money ................................................................. 2
      1.3.2. Forgery of Electronic Money ........................................................................... 3
      1.3.3. Stealing of Electronic Money ........................................................................... 3
   1.4. Structure of this Thesis work ................................................................................... 4

2. Crosscutting Technical Issues of On-line Payment Technologies ................................. 5
   2.2. Encryption and Decryption ....................................................................................... 5
      2.2.2. Encryption Techniques ....................................................................................... 6
         2.2.2.1. Symmetric Encryption .................................................................................. 7
         2.2.2.2. Asymmetric encryption ............................................................................... 7
      2.3. Hash Function .......................................................................................................... 8
      2.3.1. Hash Chains ......................................................................................................... 8
   2.4. Digital Signatures ....................................................................................................... 9
   2.5. Blind Signatures ........................................................................................................ 10
   2.6. Public Key Infrastructure [PKI] ................................................................................ 10
      2.6.1. Certificates .......................................................................................................... 11
      2.6.2. Certification Authority ......................................................................................... 11
      2.6.3. Certification Revocation List ............................................................................... 12
   2.7. Security algorithms ..................................................................................................... 12
      2.7.1. RSA .................................................................................................................... 12
      2.7.2. DES .................................................................................................................... 12
      2.7.3. Advanced Encryption Standards [AES] ............................................................. 13
      2.7.4. MD5 ................................................................................................................... 14
      2.7.5. SHA .................................................................................................................. 14
   2.8. Security and payment protocols ................................................................................. 15
      2.8.1. SSL ................................................................................................................... 15
      2.8.2. TLS ................................................................................................................... 17
      2.8.3. Kerberos ............................................................................................................ 17
   2.9. Summary .................................................................................................................... 18

3. Classification and Requirements of On-line Payment Technologies ............................. 19
   3.1. Introduction ................................................................................................................ 19
   3.2. Requirements for on-line payment systems .............................................................. 19
      3.2.1. Anonymity/Privacy ............................................................................................. 19
      3.2.2. Atomicity ............................................................................................................ 19
      3.2.3. Interoperability .................................................................................................. 20
      3.2.4. Scalability ........................................................................................................... 20
      3.2.5. Security .............................................................................................................. 20
      3.2.6. Reliability .......................................................................................................... 20
      3.2.7. Usability .............................................................................................................. 21
3.3. Classification of Current On-line Payment Technologies .......................................................... 21

4. Macro On-line Payment Systems ....................................................................................................... 23
   4.1. Introduction ...................................................................................................................................... 23
   4.2. Card Based Payment Systems ......................................................................................................... 23
       4.2.1. Credit Card Based Payment Systems .................................................................................. 23
       4.2.2. Debit Card Based Payment Systems .................................................................................. 26
       4.2.3. Stored Value Card Payment Systems .................................................................................. 28
   4.3. Electronic Check and Account Transfer Payment Systems ............................................................. 29
       4.3.1. Electronic Check Payment Systems ................................................................................... 30
       4.3.2. Electronic Account Transfer Payment Systems .................................................................. 31
   4.4. Electronic Cash Payment Systems .................................................................................................. 32
   4.5. Mobile Payment Systems ............................................................................................................... 35

5. Micro On-line Payment Systems ......................................................................................................... 41
   5.1. Micro On-line Payment Systems ..................................................................................................... 41
   5.2. Hash Chain based Micro On-line Payment Systems ....................................................................... 45
   5.3. Hash Collisions and Hash sequences Based Micro On-line Payment Systems ............................ 49
   5.4. Shared Secrete Keys Based Micro On-line Payment Systems .......................................................... 52

6. Comparison of Current On-line Payment Systems ............................................................................. 55
   6.1. Analysis of Macro On-line Payment Systems .................................................................................. 55
       6.1.1. Analysis of Credit Card Based Payment systems ............................................................... 56
       6.1.2. Analysis of Debit Card Based Payment Systems ............................................................... 59
       6.1.3. Analysis of Stored Value Payment Systems ...................................................................... 60
       6.1.4. Analysis of Electronic Account Transfer Payment Systems ........................................... 61
       6.1.5. Analysis of Electronic Cash Payment Systems ............................................................... 61
       6.1.6. Analysis of Electronic Check Payment Systems ............................................................. 64
       6.1.7. Analysis of Mobile Payment Systems .................................................................................. 65
   6.2. Analysis of Micro On-line Payment Systems ................................................................................... 66
   6.3. Comparison of Macro and Micro payment Systems ...................................................................... 69

7. Conclusion ........................................................................................................................................... 73

References .............................................................................................................................................. 75

Appendix & Glossary ............................................................................................................................... 79
List of Figures

Figure 2.1: Encryption and Decryption Mechanism................................................................. 5
Figure 2.2: The Mechanism in Digital Signatures................................................................. 9
Figure 2.3: General Format of Certification........................................................................... 11
Figure 2.4: General Structure of Certification Authority....................................................... 11
Figure 2.5: A Digital Envelope......................................................................................... 13
Figure 2.6: Security with SSL............................................................................................. 15
Figure 2.7: Communication in SSL for Authentication......................................................... 16
Figure 4.1: Credit Card Payment System Transactions....................................................... 25
Figure 4.2: Debit Card Payment System Transactions......................................................... 27
Figure 4.3: Stored Value Card Payment System Transactions.............................................. 29
Figure 4.4: Electronic Check Payment System Transactions............................................... 30
Figure 4.5: Electronic Account Transfer Payment System Transactions............................... 32
Figure 4.6: Electronic Cash Payment System Transactions................................................ 33
Figure 4.7: Mobile Payment System Transaction................................................................ 37
Figure 4.8: Generic Operation in a Mobile payment system with 3 interacting parties......... 38
Figure 5.1: Micro On-line Payment System Transactions..................................................... 42
Figure 5.2: Consumer initiated and Consumer acknowledged Micro On-line payments........ 43
Figure 5.3: Provider initiated and Provider acknowledged Micro On-line payments.............. 43
Figure 5.4: Jointly initiated and double acknowledged Micro On-line payments................... 44
Figure 5.5: Hash Chain Based Micro On-line Payment System Transactions......................... 46
Figure 5.6: Hash Collisions and Hash sequences Based Micro On-line Payment System
  Transactions.................................................................................................................. 49
Figure 5.7: Shared Secrete Keys Based Micro On-line Payment System Transactions......... 53
1. Introduction to On-line Payment Technologies

1.1. What is On-line Payment?
“On-line payment is a form of financial exchange that takes place from payer to beneficiary using an electronic means of payment in an on-line environment”[1]. E-commerce provides the capability of buying and selling products, information, services on the Internet and other on-line environments. The development of new types of E-commerce purchase relationships and business models has created the need for new ways of money exchange and new on-line payment technologies.

1.2. Motivation for On-line Payments
The most common and simplest of all payment methods is paying cash by hand. It can easily be transferred from one person to another and there are no transaction charges levied when a payment is made, which is a favorable feature in the case of low value payments. But cash payment transactions involve a lot of security and maintenance related concerns. Some of the concerns are, replacing the worn out currency with new ones, printing, maintaining, transferring them with a lot of security and the risk of counterfeit currency.

The growth of Internet in the recent years, has created an electronic marketplace for goods and services. This virtual marketplace offers not only tangible goods but also intangible goods such as knowledge, executable programs, images, music and even videos. Most of these intangible products are delivered electronically. As in any trading activity, the issues of safety and reliable money exchange are essential. The development of a new type of E-commerce purchases, transactions and business Models [B2B, B2C, C2C] have created the need for new ways of money exchange between the interested parties [2].

A large number of new Internet-based payment systems have been invented in recent years. A good number of those On-line payment systems disappeared after failing to gain the acceptance of the users. Most of these methods need some sort of trusted third party service to serve as an...
Comparison of Current On-line Payment Technologies

intermediary to the transactions. The main advantages of on-line payment methods are convenience and efficiency. As the on-line payment methods are largely unregulated, the rights of the parties involved in the transaction are controlled by the terms and conditions of the service provider and may not be by the government.

1.3. Security Concerns of On-line payments

On-line payment technology is a new payment instrument for various types of E-commerce purchasing, transaction and business Models [B2B, B2C, C2C]. Majority of current on-line payment methods allow monetary value to be represented in the electronic form and transferred from one entity to another across computer networks with much security and little chance for fraud. Majority of the current existing on-line payment methods are designed to securely allow payments ranging from fraction of a dollar to thousands of dollars. Even though the on-line payment companies use different kinds of software and/or hardware security applications for the security and reliability of their on-line payment methods, the payment technologies still encounter various security related problems because of the nature of the money representation [3]. Some of the main security concerns of On-line payment technologies are

- Double Spending the Electronic Money
- Forgery of Electronic Money
- Stealing of Electronic Money

1.3.1. Double Spending Electronic Money

Electronic money is nothing but electronic form of data [or numbers] representation and it can be copied easily and arbitrarily. If some one tries to spend the copied electronic money repeatedly, that is called double spending and the on-line payment technology should apply some mechanism that detects and prevents double spending. Like in the paper based money, the financial organizations cannot record all the information of electronic money [serial numbers, who spent the money and when etc], which they issue. While providing one of the desirable qualities of on-line payment technologies, anonymity, the payment technology organizations face more security related problems as they can't trace the people, who spent the money. To ensure that the same electronic money with the serial number is not spent more than once, the money issuing organization must record every electronic coin that is deposited back to that organization. This can make the database
of the money issuing organization, very large and unmanageable[4].

1.3.2. Forgery of Electronic Money
In general, it is quite difficult to forge traditional money as the currency notes must have special, expensive or difficult to forge physical features [special paper, print or color, emblems, water marks etc]. Since, Electronic money is nothing but electronic form of data [or numbers] representation and it does not have to satisfy specific properties, or if the properties are so simple that it is easy to generate many bit strings that satisfy them, acceptable electronic money (forgeries) can be produced practically by anyone using an unauthorized principal. In an off-line payment system, there is no possibility to verify in real time whether, the electronic money was issued by an authorized on-line payment organization. Consequently, off-line payment systems must have some protection against forged coins.

1.3.3. Stealing of Electronic Money
Since, electronic money is nothing but electronic form of data [or numbers] representation and it can easily be stolen (picked up by eavesdroppers) and spent by unauthorized principals, if they are not encrypted. If payers are anonymous, there is no way for a payee to differentiate between a legal owner and a thief using stolen electronic money. There are, however, some mechanisms to prevent stealing of electronic money, and they are used to implement the corresponding payment security service[5].

In addition to the above security concerns, the following security risks can also play a significant role in the failure of any on-line payment system. They are

- Outsiders eavesdropping on the communication line and misusing the collected data (e.g., credit card numbers).
- Hackers sending forged messages to authorized payment system participants in order either to prevent the system from functioning or to steal the assets exchanged (e.g., goods, money).
- Dishonest payment system participants trying to obtain and misuse payment transaction data that they are not authorized to see or use.
1.4. Structure of this Thesis work

The second chapter, “Crosscutting Technical Issues of On-line Payment Technologies”, includes a short introduction of various security and cryptographic fundamentals, which are necessary to understand this thesis work.

The third chapter, “Classification and Requirements of Current On-line Payment Technologies”, includes various requirements that have to be satisfied by an on-line payment technology and the classification of on-line payment technologies, based on their mode of operations.

The fourth chapter, “Macro On-line Payment Systems”, includes description of various macro on-line payment systems, their operations, technical issues and some example systems of each macro on-line payment systems.

The fifth chapter, “Micro On-line Payment Systems”, includes description of various micro on-line payment systems, their operations, technical issues and some example systems for each micro on-line payment system.

The sixth chapter, “Comparison of Current On-line Payment Systems”, includes an analysis of various on-line payment systems and comparison of current on-line payment methods.

The seventh chapter, “Conclusion”, summarizes the various on-line payment systems and figures out why the credit card based payment system is the most favorable and popular on-line payment system.
2. Crosscutting Technical Issues of On-line Payment Technologies

2.1. Introduction
The on-line payment technologies rely on a number of other technologies and policy issues to provide the reliable service to the users. Cryptography is the most prominent among them. Since, cryptography is such an important part of an on-line payment, it is worth discussing some of the cryptographic technical issues. This chapter briefly covers a basic introduction to the essential cryptographic techniques necessary to understand, how the on-line payment technologies work.

2.2. Encryption and Decryption
In cryptographic terms, a message in the human readable form is referred to as plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption and the resulting message is referred to as ciphertext. Encryption ensures that the information is hidden from others for whom it is not intended for. The process of reverting ciphertext to its original plaintext is called decryption[7].

![Encryption and Decryption Mechanism](image)

Figure 2.1: Encryption and Decryption Mechanism
2.2.1. Basic Principles of Encryption

The strength of any encryption systems depends on how strongly they are following the basic principles of encryption. Some of the basic principles of encryption are[7]

- Authentication
- Non-repudiation
- Verification
- Privacy

Authentication

This is the process of verifying the true sender of a ciphertext and verifying that the text of the message has not been altered. The general way to perform authentication is applying private key to encrypt a message and decrypt the encrypted message with the public key. This process guarantees that only the authenticated user can have the encrypted message. A message is signed only once with digital signatures [It has been discussed in the next section of this chapter] but it may be verified many times in the course of On-line payments.

Non-repudiation

This is the quality of a secure system that prevents anyone from denying that they have sent certain data. Here the communication system should be fault tolerant. Security systems like Kerberos[It has been discussed in the next section of this chapter] provide non-repudiation as the server keeps a record log of every transaction and the user can't deny that he or she has not accessed the server.

Verification

This is the process which ensures that a certain message can be trusted. This is possible because verification has the ability to identify and authenticate a particular encrypted communication. A message should be identified and authenticated before it can be trusted completely.

Privacy

This is the process which shields the communication between the authorized parties from the other parties. The privacy level is high in strong encryption systems than in the weak encryption systems.

2.2.2. Encryption Techniques

There are two types of encryption techniques that exist today. They are

- Symmetric Encryption
- Asymmetric Encryption
2.2.2.1. Symmetric Encryption

They are mainly used for achieving confidentiality, to authenticate the integrity and origin of data. They can also support limited non-repudiation. In this encryption technique, the same secret key is used both for encryption and decryption. Because of this the algorithms used in symmetric cryptographic are often referred to as secret key algorithms. Before transferring any data between two participants, they have to decide on which algorithm they use and have to make sure that they use the same secret key. The distribution of secure keys is a challenging task and it should be performed through a secure trusted courier. Symmetric encryption is fast and can be implemented easily as long as the number of participants are low. If the number of participants increase, then so does the number of key pairs and it is very difficult to manage the system. One solution to this problem is asymmetric encryption. The most popular symmetric encryption systems is Data Encryption Standard [DES] [7].

2.2.2.2. Asymmetric encryption

In asymmetric encryption, each participant needs to have one pair of keys. They are public key and private key. The public key is widely published and distributed and the private key is protected secretly by each participant. There are two different ways to use this key pair.

In the first approach, Sender encrypts the data with the receiver's public key and the receiver will decrypt the message with his own private key. But in this process the authentication of sender is not very clear as every body has the access to the public key.

In the second approach, the sender encrypts the data with his own private key and the receiver can decrypt it with the sender’s public key as it's available to all receivers. But the problem with this method is, anyone can decrypt the message from the sender as every one access the sender’s public key. The solution to this problem is to use a combination of sender's private key and receiver's public key. In this procedure the sender can encrypt the data with the receiver's public key and re-encrypt the already encrypted data with his own private key. The receiver uses the appropriate keys to decrypt the data [receivers private key first and the senders public key next].As the public key is openly available, the users should keep their private keys securely. The most commonly used asymmetric algorithm is RSA [7].
If the above encryption techniques are implemented in Software then Symmetric Encryption [which uses DES] is 100 times faster than Asymmetric Encryption [Which uses RSA]. If they are implemented in hardware, Symmetric Encryption [which uses DES] is 1,000 to 10,000 times faster than Asymmetric Encryption [Which uses RSA] [8].

2.3. Hash Function

The hash function $H$, takes a plaintext of any length and produces a fixed length output known as message digest or hash value [MD=$H(m)$]. If the input information is changed even by just one bit then the hash function produces a different output. The basic requirements for a cryptographic hash functions are:

- The input can be of any length.
- The output has a fixed length.
- $H(x)$ is relatively easy to compute for any given plaintext $x$.
- $H(x)$ is one-way.
- $H(x)$ is collision-free.

A hash function $H$ is said to be One-way, if it is computationally impossible to calculate the original message $(m)$ from the given hash value $(h)$. Here $H(m) = h$.

A hash function $H$ is said to be collision-free if it is computationally impossible to produce the hash values such that $H(m_1) = H(m_2)$ from two messages $m_1$ and $m_2$, $m_1$ is not equal to $m_2$.

The common use of hash function is to store passwords. When the user enters his password it would be transformed by a hash function and compared with the hash value. Only if both those values match, the system lets the user to log on. The main role of a cryptographic hash function is in the provision of digital signatures. Digital time stamping can be achieved with the use of hash functions as a digest can be made public without revealing the contents of the document from which it is derived from. So one can get a document “time stamped” without revealing the contents to the time stamping service [8].

2.3.1. Hash Chains

A hash chain of length $n$ is constructed by applying a hash function $n$ times to a random value labeled $x_n$. The value $x_n$ is called the root value of the hash chain. A hash chain derived using a
hash function $h$ recursively can be represented as:

$$h_n(y) = h(h_{n-1}(y))$$

$$h_0(y) = x_n$$

Where $h_n(y)$ is the result of applying a hash function repeatedly $n$ times to an original value $y$. The final hash value, or anchor, of the hash chain after applying the hash function $n$ times is $x_0 = h_n(x_n)$. The hashes are numbered in increasing order from the chain anchor $x_0$, so that $h(x_1) = x_0$ and $h(x_2) = x_1$. Each hash value in the chain can provide a single user authentication. The user releases $x_1$ for the first authentication, $x_2$ for the second and so on. The server only has to apply a single hash function to verify that the received value hashes to the previous value. The user only needs to store $x_n$ from which the rest of the chain can be re-computed. The final hash $x_0$ of a chain may need to be securely swapped across a network [9].

2.4. Digital Signatures

Digital signatures serve the same purpose as the handwritten signatures, that is authentication of its creator. In addition to authentication, Digital signatures provide data integrity, non-repudiation [if the sender sends the message along with the digital signature the he can't deny that he has not sent the information ][7].

![Figure 2.2: The Mechanism in Digital Signatures](image)

As depicted in the figure 2.2, Information is encrypted using the sender's private key and it would be decrypted using the public key of the sender. So this procedure guarantees the authentication of the sender. As long as a secure hash function is used, there is no way one copy signature and alter a signed message on the way. If the hash function is applied on a message with a secret key added,
the hash value is called a message authentication code [MAC].

2.5. Blind Signatures
D. Chaum, proposed this Cryptographic mechanism. A blind signature is a special kind of digital signature. Unlike the regular digital signature, a blind signature does not reveal the content of the document fully to the person, who signs on it. Blind signatures assure the receiver that the transmission is authentic and reliable. In the On-line payment technologies, Blind signature guarantees both payer anonymity and hiding payment transaction details by using RSA signature[7].

2.6. Public Key Infrastructure [PKI]
Public key infrastructure can be described as a combination of hardware and software, protocols and procedures, to secure transactions over public networks [34]. It is based on the idea that an individual will generate a key pair, private and public key. The most fundamental purpose of a public key infrastructure is to provide the following basic security services

- **Authentication:** This ensures that all the parties involved in the transactions, messages and their transmissions are authentic.
- **Data Integrity:** This ensures that the data is not changed in the transmissions, either accidentally or maliciously
- **Non-repudiation:** This ensures that a trusted third party can verify the integrity and origin of the data. It also ensures some sort of communication between the sender and receiver's for proper deliver of the message from the genuine party.
- **Confidentiality:** This ensures that only authorized parties can access the information.

One of the important aspects of the PKI is the reliable distribution of the public keys [in asymmetric encryption] and to ensure that it needs a trusted Third party [TTP]. The most common components of PKI are

- Certificates
- Certificate Authority(CA)
- Certification Revocation List(CRL)
2.6.1. Certificates
A certificate is a digital document that binds a public key to its authorized owner. The certificate can ascertain user identity of the public key. The TTP signs this certificate using his private key and this process guarantees that the public key is associated with the named user [4]. The general format of the certificate can be

![Figure 2.3: General Format of Certification](image)

<table>
<thead>
<tr>
<th>Subject [User Identity]</th>
<th>Public Key</th>
<th>Validity period</th>
<th>Identity Of TTP Fields</th>
<th>Signature Of TTP</th>
</tr>
</thead>
</table>

2.6.2. Certification Authority
To ensure the user that he has received the genuine public key from a genuine sender, a trusted third party [TTP] as a certifying authority is needed. Trusted third parties [TTP], which issue the certificates, are referred as certification authorities. When the number of users becomes large then it's unlikely that a single CA can server every user. So that there are many independent CA's and they are organized into a hierarchy [5].

![Figure 2.4: General Structure of Certification Authority](image)

In this hierarchy, every CA has a key pair and the private key is stored with extreme care. If the
CA's private key is known to attacker then he can produce fake certificates and it will lead to the
total collapse of the CA hierarchy. Certificates from different CA's should be valued differently as
different CA's can offer different levels of trustworthiness.

2.6.3. Certification Revocation List
Certification revocation list maintains all the lost or destroyed private keys. Those keys will be
maintained in the list as long as they are active. They will be removed from the list, once they reach
their expiration date. Every PKI system should prepare to prevent the misuse of keys lost or
destroyed. If there is any misuse of private keys then the concerned CA’s should contact each other
immediately and the corresponding public keys should be revoked and put on the certification
revocation list[CRL] to prevent any further misuse of keys.

2.7. Security algorithms
The following algorithms are some of the most commonly used security algorithms in the
cryptographic methods.

2.7.1. RSA
RSA stands for Rivest, Shamir, and Adleman, who invented this algorithm in 1978[44]. RSA is the
easiest public-key algorithm which works for encryption as well as for digital signatures so far.
RSA algorithm security technique is based on the factoring of very large primes [at least 100 to 200
digits].

Generating security key in RSA:
For every pair of secret keys, the user has to take two large prime numbers \( p \) and \( q \). The two primes
are multiplied and the product \( n \) is called modulo. Another number \( e \) is chosen, which is relatively
prime to \((p-1)(q-1)\), which means that \( e \) and \((p-1)(q-1)\) have no common factors except 1, and \( e \) is
less than \( n \). Another number \( d \) is chosen that is the inverse of \( e \), which means that \( ed = 1 \mod (p-1)(q-1) \).
Now we have the two required key pairs. Public key \((n, e)\) and the private key \((n, d)\). The
initial two prime numbers should be kept secret as the whole calculation procedure depends on
them and some one can deduct the value of \( d \) from them.
2.7.2. DES

DES is a secret-key or symmetric-key cryptographic algorithm. The DES can be used for both encryption/decryption and authentication. DES is based on an algorithm developed at IBM in the early 1970s. DES is a block cipher algorithm, which means that it operates on a single chunk of data at a time. The security of DES is based not on the secrecy of its encryption algorithm but on the secrecy of the key used to encrypt a given message. In general, the key length is 56-bit and which is not sufficient to safeguard against brute force attacks. To strengthen it further, triple-DES or 3DES cryptographic system has been developed. The 3DES is exactly the same as the DES except that the data is going through the cipher system three times by using two different keys. When used together, RSA and DES provide a secure digital envelope for sending encrypted messages as RSA provides two functions which DES does not provide, they are

- Secure key exchange without prior exchange of secret keys.
- Digital signatures.

The general combination of RSA and DES can be combined as follows [35]

The message is encrypted with a random DES key and the DES key is encrypted with RSA

- The DES encrypted message and the RSA-encrypted DES key are sent together as a secure digital envelope.
2.7.3. Advanced Encryption Standards [AES]

The advanced Encryption Standards [AES] specifies a FIPS [Federal Information Processing Standards] approved symmetric 128-bit block data encryption algorithm that can be used to secure sensitive electronic data. AES is a symmetric block cipher algorithm that can encrypt and decrypt information. The AES applications emphasizes both hardware and software implementations equally. AES works at multiple network layers simultaneously [32].

With a key size of only 56 bits, it was becoming increasingly possible to break a DES-encryption message simply by cycling through all of the possible keys. In response to this challenge, National Institute of Standards and Technology [NIST, USA] selected the Rijndael algorithm developed by Joan Daemen and Vincent Rijmen among the five security algorithms it hand considered [MARS, RC6, Rijndael, Serpent and Twofish]. NIST considered Security, Cost, efficiency, ease of implementation and flexibility in the selection of Rijndael algorithm among these five algorithms [7].

AES [Rijndael] has become the encryption algorithm of choice for all new developments, which requires a high degree of data security with added flexibility of variable key and data block sizes. The AES [Rijndael] algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. The implementation of AES, in software and/or hardware is designed to protect digital information [video, voice, images and data] from attacks or electronic eavesdropping [34].

2.7.4. MD5

The MD5 algorithm is one of the series (including MD2 and MD4) of the message digest algorithms developed by Ron Rivest. It involves appending a length field to a message padding up to a multiple of 512-bit blocks. Each of these 512-blocks is then fed through a four round process involving rotation and range of boolean operations, which produces a chaining value that is input to the processing of the next 512-bit block. The hashed output is the 128-bit chaining value, which is produced in processing the last block of the message [8].
2.7.5. SHA
NIST released a series of cryptographic standards in 1993, one of which specified the secure hash algorithm [SHA]. It is based quite heavily on the work of Ron Rivest in the MD series of algorithms. The message is first padded as with MD5, and then fed through four rounds, which are more complex than those used in MD5. The chaining value passed from one round to the next is 160 bits in length, which means that the resulting message digest is also 160 bits[8].

2.8. Security and payment protocols
In on-line payment technologies, secure communication between various participants is very important and there should be proper protection against eavesdropping, tampering and forgery. Clients and servers are able to authenticate each other to establish a secure link across the Internet or Intranet to protect the information transmitted. There are some security protocols which supports secure connection between the genuine parties.

2.8.1. SSL
Secure Socket Layer [SSL] is the Internet security protocol to be used to secure any communication taking place between applications, which communicates across a “socket” interprocess communication mechanism. It was developed at Netscape Corporation in 1994[35]. The main motivation behind this protocol design is Internet security.

![Figure 2.6: Security with SSL](image)
As the figure 2.6, SSL adds security by acting as a separate security protocol, inserting itself between the HTTP application and TCP. SSL requires very few changes in the protocols above and below as it acts as a new protocol. In the on-line payment technologies, proving the authentication of the parties involved in the transaction is very much important. SSL supports the authentication in the following way.

From the figure 2.7, the Communication in SSL for Authentication, can be summarized in the following steps:

**Step 1:** Client sends ClientHello message proposing SSL option.

**Step 2:** Server responds with ServerHello selecting the SSL option.

**Step 3:** Server sends its public key certificate in Certificate message.

**Step 4:** Server concludes its part of negotiation with ServerHelloDone message.

**Step 5:** Client sends session key information (encrypted with server's public key) in ClientKeyExchange message.

**Figure 2.7:** Communication in SSL for Authentication
**Step 6:** Client sends ChangeCipherSpec message to activate the negotiated option for all future messages it will send.

**Step 7:** Client sends finished message to let the server check the newly activated options

**Step 8:** Server sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.

**Step 9:** Server sends finished message to let the client check the newly activated options.

### 2.8.2. TLS

TLS is based on the secure socket Layer Version 3.0 and it is considered to be an improvement to SSL 3.0. It was released in January 1999 to create standards for private communication. This protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery\[11\]. The goals of this protocol are cryptographic security, interoperability, extensibility and relative efficiency. These goals are achieved through the implementation of TLS protocol on two levels:

- TLS Record Protocol
- TLS Handshake Protocol

The TLS Record Protocol negotiates a private, reliable connection between the client and the server. It uses symmetric cryptographic keys to ensure a private connection, though it can be used without encryption. This connection is secured through the use of hash functions generated by using a Message Authentication Code [MAC].

The TLS Handshake Protocol allows authentication of the communication between the server and the client. This protocol facilitates the server and the client to agree upon an encryption algorithm and encryption keys, before the selected application protocol begins to send data.

### 2.8.3. Kerberos

Kerberos is a network authentication protocol developed as part of MIT's project Athena [43]. Kerberos provides a centralized authentication mechanism for restricted and authenticated network services over untrusted networks. It allows users to authenticate servers and servers to authenticate users easily. The main goals of this protocol are [45]
Comparison of Current On-line Payment Technologies

- **Secure**: Network infrastructure should not provide sufficient information to compromise the system. So that no eavesdropper should be able to gather enough information to impersonate a Kerberos user.

- **Reliable**: The system should be highly reliable and should be distributed.

- **Transparent**: The user should only have to perform a single, simple, initial authentication and all subsequent authentications are invisible.

- **Scalable**: The system should be able to support large number of users and servers, generally through distribution and modularization.

Kerberos basically works by centrally authenticating a user, It gives him an authentication ticket which can be used to get other individual access tickets. The user first authenticates himself to the Authentication Server[AS] and then the server sends the user a Ticket Granting Ticket[TGT]. This TGT is encrypted and the user can decrypt it. By the use of Ticket Granting Service[TGS], the submission of passwords in plain text over the network can be prevented and it increases the security level. For every service the user wants to use, the user requests a service ticket from the Ticket Granting Server[TGS]. So the user can use this service ticket that authenticates and verifies them with the desired service.

2.9. Summary

In On-line payment technologies, to provide a secure and reliable service to the customer, there should be an authenticated communication between the parties concerned. Various encryption and decryption techniques [Public Key Encryption, Private Key Encryption] together with signature mechanisms help the users to achieve this goal. To provide a secure connection between the genuine parties, security protocols will be handy [SSL, TSL and Kerberos].
3. Classification and Requirements of On-line Payment Technologies

3.1. Introduction
This chapter presents some of the requirements of on-line payment technologies, which are necessary to provide a reliable service to the customer in an e-commerce environment. This chapter also tries to classify current on-line payment methods on the bases of their method of payment and their applications [small payments or large payments].

3.2. Requirements for on-line payment systems
The success or failure of any on-line payment systems, depends not only on technical issues but also on users acceptance. The users acceptance depends on a number of issues such as advertisement, market position, user preferences etc. So when some one discuss about the characteristics of on-line payment technologies, they should not only think about technical issues but also about user acceptance related issues[6].

3.2.1. Anonymity/Privacy
Anonymity suggests that the identity, privacy and personal information of the individuals using the on-line payment methods should not be disclosed. In some on-line payment methods, it is possible to trace the individual’s payment details. In case of purchases using Debit Card, it is possible to find out the purchase details as that information is registered at the vendor and the bank's databases. So some on-line payment systems like Debit cards are not anonymous systems. In some other payment systems, anonymity can be weak as the efforts to get the purchase details of the user can be more expensive than the information itself. There are privacy laws in several countries to guarantee the privacy of the user and protect the misuse of personal information by the financial institutions.

3.2.2. Atomicity
Atomicity guarantees that either the user's on-line payment transaction is completed or it does not take place at all. If the current on-line payment transaction fails then it should be possible to recover the last stable state. This feature resembles the transactional database systems, in which either a
transaction is committed or rolled back.

3.2.3. Interoperability
In On-line payment Technologies, different users prefer different payment systems. The different payment systems use different kinds of currencies and the payment systems should support interoperability between them. If a payment system is inter operable, then it is open and allows other interested parties to join without confining to a particular currency. In the real life situation, there should be some sort of mutual agreement between various on-line payment systems to provide the interoperability. Interoperability can be achieved by the means of open standards for data transmission protocols and infrastructure. An interoperability system can gain much acceptance and high level of applicability than individually operating payment systems. Because of the rapid technological changes, it's not always easy to get interoperability between various payment systems.

3.2.4. Scalability
As the on-line payment methods are getting more and more acceptance of the users, the demand for on-line payment infrastructure will also be increasing rapidly. Payment systems should handle the addition of users without any performance degradation. To provide the required quality of service without any performance degradation, the payment systems need a good number of central servers. The central servers are needed to process or check the payment transactions. The growing demand for the central servers, limits the scalability of the on-line payment systems.

3.2.5. Security
Security is one of the main concerns of the on-line payment methods and it is one of the crucial issues which decide the general acceptance of any on-line payment methods. Internet is an open network without any centralized control and the on-line payment systems should be protected against any security risks to ensure a safe and reliable service to the users. When users are paying on-line they want to be sure that their money transaction is safe and secure. On the other hand, banks and payment companies and other financial institutions want to keep their money, financial information and user information in a secure manner to protect it against any possible misuse.
3.2.6. Reliability
As in any other business activity, even in on-line payment methods, the user expects a reliable and an efficient system. Any on-line payment system would fail, despite of it's advanced technological features, if it fails to get the users acceptance and pass their reliability tests. There are many reasons, which can make the system unreliable to the users. Some of them are Security threats, poor maintenance and unexpected breakdowns.

3.2.7. Usability
Usability is an important characteristic of an interactive product like on-line payments. On-line payment systems should be user friendly and easy to use. Any on-line payment system with complicated procedures, complex payment process and other associated complications with the payment environment, can't get users acceptance. Poor usability of a web shopping or a payment method could also discourage on-line shopping. To make the on-line payments simple and user friendly, some of the on-line payment systems allow the users to make payments with minimum authorization and information inputs.

3.3. Classification of Current On-line Payment Technologies
The money has been changing from one form to another form since centuries. Ancient representations of whale's teeth to modern electronic money [Money is not represented in the physical form but in an electronic form in a computer system]. The payment methods have also been changing accordingly from one form to another form; ancient barter system to modern on-line payment system. With the advancements in the Internet technology, many on-line payment technologies have been developed in these days. Many of these on-line payment methods are developed on the basis of existing payment instruments and others are developed on the basis of new form of value representation and exchange. Majority of current on-line payment methods allow monetary value to be transferred from one entity to another across computer networks with much security and little chance for fraud[10].

Majority of the current existing on-line payment methods are designed to allow secure payments ranging from fraction of dollar to thousands of dollars. For the security and reliability of their on-line payment methods, different companies use different kinds of software and/or hardware security
Comparison of Current On-line Payment Technologies

applications. Current On-line payment systems are mainly divided into two systems, depending on the value of money transactions, processing time, computational requirements, security issues and usability requirements. They are

- Macro On-line Payments Systems
- Micro On-line Payments Systems

Macro On-line payment systems, support payments approximately ranging from one dollar to several thousand dollars. These payment methods involve minimum transaction overheads imposed by issuing banks or companies. These payment systems assure authenticity and privacy to the users. The security requirements are more rigorous in these payment systems because of huge money transactions. This payment system have been discussed in detail, in the chapter 4.

Micro On-line payment systems support frequent transfers of very small amounts as small as a fraction of dollar [even less than a cent]. Because of the small amounts involved, higher efficiency can be achieved by slightly relaxing the security mechanism. Micro on-line payment methods aim at providing a reasonable level of security with more economical usage of computer resources and time. This payment system have been discussed in detail, in the chapter 5.
4. Macro On-line Payment Systems

4.1. Introduction
Macro On-line payment systems are designed to allow secure on-line payments ranging from one US dollar to several thousand US dollars. Macro on-line payment systems are modeled on real world payment instruments and have a minimum transaction overheads imposed by the issuing banks. These transactional overheads and heavy usage of computationally expensive cryptographic operations prevent these payment systems to be used for the payment of small amounts [amounts ranging from a fraction of a US Dollar to one US dollar]. Some of the popular macro on-line payment systems are mentioned below. They are [8]

- Card Based Payment Systems
- Electronic Check and Account Transfer Payment Systems
- Electronic Cash Payment Systems
- Mobile Payment Systems

4.2. Card Based Payment Systems
There are variety of on-line payments available now. Some of them are Card-based while others are electronic instruction oriented. In general, these payments link to an existing account relationship to a financial institution for both payer and payee. There are three widely used Card-based on-line payment systems. They are[36]

- Credit Card Based Payment Systems
- Debit Card Based Payment Systems
- Stored Value Card Based Payment Systems

4.2.1. Credit Card Based Payment Systems
“Credit card based payment systems have payments set again a special-purpose account associated with some form of installment-based repayment scheme or a revolving line of credit. Credit cards typically have a spending limit set by the card issuer, and the interest rate levied on unpaid balance is typically many times the base lending rate”[46].
Credit-card based payment systems have been in use since the early 1960s. There are many card companies in the market, but Visa Card and MasterCard are the two major international players in this field. There are five parties involved in the credit card transaction:

- **Card Holder**
- **Merchant**
- **Issuing Bank**, which issues the credit card and operates a card account to which payments can be charged.
- **Acquiring Bank**, which handles the merchant’s receipts. A merchant who wish to accept payments must register with the acquiring bank.
- **Credit Card Network**, which is a co-operative venture between the affiliated card issuers. It links the issuing, acquiring banks and co-ordinates the exchange of information, flow of funds between them. e.g Visa Card or MasterCard.

**The functionality of Credit Card:**

When the card holder swipes his or her credit card at the point of sales terminal [POS], the information stored on a magnetic strip or a chip will be transmitted to acquiring bank in encrypted form. The acquiring bank checks the information containing Merchant’s ID, The card number, the expiry date, the credit limit and remaining credit [4].

The acquiring bank connects to the issuing bank through the network’s computer. The issuing bank transmits the account information and later transfers the funds to the acquiring bank. The issuing bank then debits the card holder’s account and reduces the balance of credit available [4].

The network [Visa Card or MasterCard] charges the issuing banks to cover its costs. The acquiring banks charge the merchants a percentage of each transaction and pay interchange fees to the issuing banks. The issuing banks charge card holders some interest on unpaid balances or an annual fee.
Figure: 4.1 Credit Card Payment System Transactions

From the figure 4.1, the Credit Card Transaction can be summarized in the following steps:

**Step1:** The Payer [Consumer] pays a Payee [Merchant] with a credit card at the POS [point of sale].

**Step2**

&

**Step3:** The Payee [Merchant] transmits the data at POS through the bankcard association’s network to the card issuer for authorization.

**Step4**

&

**Step5**

&

**Step6:** If the issuer authorizes, then the merchant receives the authorization to capture funds and the card holder accepts liability by signing the credit voucher.

**Step7**

&
Step 8: The merchant receives the payments by submitting the captured credit card transactions to its financial institution in batches or at the end of the day.

Step 9

&

Step 10: The merchant’s bank [Acquire Bank] forwards the sales draft to the bankcard Association, which in turn forwards the data to the card issuer.

Step 11: The bankcard association determines each financial institution’s net debit position and the association’s settlement financial institution coordinates issuing and acquiring settlement positions. The settlement process takes place using a separate payment network.

Step 12: The card issuer presents the transactions on the card holder’s next monthly statement.

Security of Credit Card Transactions [37]:

SSL and TLS are used to encrypt payment transaction messages, including the payment card details, sent between the payer and payee over the Internet. Here, SSL uses authentication based on asymmetric cryptography issued by trusted third party. In general, the authentication of Payee [Merchant] takes place and after the authentication process, all the messages are encrypted using symmetric cryptography. The actual cryptographic algorithms used are negotiated at connection setup. The payee verifies that card details at the time of purchase through an existing financial network.

Secure Electronic Transaction [SET], is the common proposed standard by Visa Card and MasterCard for secure on-line payments. SET suggests a hierarchy of CAs [Certification Authority] instead of a single CA, a strong public key encryption, a strong card binding mechanism and a dual signature scheme to link order and payment details together. Despite of this good feature, SET can be a burden to the payment system as it demands a large number of computationally expensive signatures and messages to complete a single transaction. One improvement in the direction is the design of lighter version of SET, which reduces the computation time and resources significantly [37].
4.2.2. Debit Card Based Payment Systems

Debit-card payment systems are linked to a checking or saving account at a financial institution. Debit cards look like credit cards or Automated Teller Machine [ATM] cards but this type of payments can be considered as a paperless check. While credit card is a way to “pay later”, a debit card is a way to “pay now”. Debit cards are either on-line [PIN-based] or off-line [signature-based] [8].

On-line debit cards, use a PIN for customer’s authentication and on-line access to account balance information. They are usually enhanced ATM cards and they work in the same manner of an ATM transaction. The financial institutes authenticate customer by matching the PIN with the account number directly through the Payee [Merchant] terminal. Here the debit card transaction used the same Electronic Fund Transfer [EFT] that handles the ATM transactions.

Off-line debit cards, authenticate the customer through a written signature. Here the transaction process is more over like the credit card transactions and through the back card networks and all the card transactions settle at the end of the business day.

![Debit Card Payment System Transactions](image)

**Figure 4.2:** Debit Card Payment System Transactions
From the figure 4.2, the Debit Card Transaction can be summarized in the following steps

**Step1:** The Payer [Consumer] enters a PIN to authorize the transaction.

**Step2**

&

**Step3:** The Payee’s [Merchant’s], financial institution requests authorization from the Consumer’s financial institution through the EFT network.

**Step4:** The consumer’s financial institution verifies funds and debits of the consumer.

**Step5:** The EFT network authorizes the purchase.

**Step6:** The EFT, determines the net debit and credit positions of the participating financial institutions and settle their positions using the ACH [account clearing house].

**Step7:** The merchant receives the transaction amount, net of applicable fees and other expenses assessed by the acquiring financial institutions and other intermediaries to the transaction.

**Step8:** At the end of the business day. The issuing and acquiring financial institutions establish a net settlement of all the transfers between them using ACH [account clearing house].

### 4.2.3. Stored Value Card Payment Systems

Stored value cards are cards with magnetic stripes or computer chips that are charged with fixed values that can be spent or transferred to individuals or merchants in a manner that is similar to spending paper money. In addition to cash, a stored value card can allow other items of value, such as purchase points, phone time etc. Some stored value cards may also be smart cards if they contain an integrated microchip. The integrated chip can store value and perform other functions such as consumer authentication. Stored value cards can come in the form of cash-replacement cards, phone cards, gift cards etc. These cards can store one-time fixed amounts of electronic money or they can interact with the loading devices that allow increase to the available amount [38]. These cards are typically used for low-value purchases.
Figure 4.3: Stored Value Card Payment System Transactions

From the figure 4.3, the Stored Value Card Transactions can be summarized in the following steps:

**Step1:**

**Step2:** The consumer purchases a stored value card.

**Step3:**

**Step4:**

**Step5:** When the consumer pays for the goods or services with the stored value card, electronic notations or tokens transfer from the card to the merchant’s cash register.

**Step6:** The merchant contacts the computer network of the financial institution that Issues the stored value card and presents the tokens for payment.

**Step7:** The network notifies the consumer’s financial institution to pay the appropriate sum to the merchant’s financial institution and net settlement occurs at the end of the business day.

**4.3. Electronic Check and Account Transfer Payment Systems**

Paper-based payments using a check are still highly popular in many nations. These trends are changing rapidly because the paper-based checks are expensive to process and the average cost for check is quite high in case of bounced checks. The basic idea of Electronic check payment system
is, the electronic document can substitute paper based check. The public key cryptographic signature can replace handwritten signature without creating a new payment instrument with new legal, commercial and regulatory polices. The Electronic Check and account transfer payment systems have all the properties of a check-based payment with more advanced and effective electronic verification features[8].

4.3.1. Electronic Check Payment Systems

In these systems, each check is usually generated and digitally signed by the payer before being passed across the network to the payee for verification. The payee endorses the check by applying a further digital signature before sending it to the network bank. Existing financial networks can be used to clear the electronic check between the payer and payee's bank. To ensure the availability of the funds during a purchase, the check should be cleared on-line. The digital signatures ensure that each party is fully identified. Electronic Exchequers have a similar payment model to payment card schemes. A digitally signed check is transferred through the payee to an acquiring bank for authorization and clearing with the issuing bank. Like, in on-line credit card payments, digital signature creation and verification is required by all parties. Money will be drawn from the payer's account at the time of purchases or even after that [39].

Figure: 4.4: Electronic Check Payment System Transactions
From the figure 4.4, the Electronic check transactions can be summarized in the following steps

**Step1:** The payer sends an Electronic Check with all the information required and cryptographic signature.

**Step2:** The Payee sends back an invoice after receiving the Electronic check.

**Step3:** The payee verifies the payer's signature and sends it to the payee's bank in the form of Secure Envelope which is having the check details.

**Step4:** The Payee's bank verifies the payer's and payee's signatures and sends electronic check for the ACH check clearing. It credits the payee's account.

**Step5:** The payer's bank verifies the payer's signature and debits the payer's account and sends an E-mail statement to the payer.

In general, Electronic checks are written in Financial Service Markup Language [FSML], as FSML supports data structures and cryptographic signatures which are needed for electronic checks. X.509 certificates are used with electronic checks to provide the verifiers of public key signatures with the signer's public signature verification key. X.509 is issued to the customers at the time of opening an account with the bank. The cryptographic signatures are sufficient to secure the electronic checks against fraud as they are ensuring message integrity, authentication and non-repudiation. For more confidentiality, encrypted email can be used between the payer and payee or between the payee and the bank [8].

### 4.3.2. Electronic Account Transfer Payment Systems

It is an alternative payment method to electronic checks and Card-based payment systems. In this payment method, the payer authorizes funds to be transferred from one account to another, most of the time at the same network banks. These payment systems support not only customer-merchant payments but also customer-customer payments. Accounts of individuals can be funded using card-based payments [credit card or debit card] or transferring of funds form a regular bank account. The communications with the bank is well protected with SSL and authentication is based on password. The password should reasonably be strong enough to guard against any possible attacks. Papal, Yahoo Pay Direct and Prepay are some of the commercial applications of Account transfer payment systems [8].
From the figure 4.5, the Electronic Account Transfer payment system transactions can be summarized in the following steps:

**Step1:** Select account payment system.

**Step2:** Redirect to payment system with transaction details.

**Step3:** Payment authorization over SSL.

**Step4:** Redirect to merchant with payment indications.

**Step5:** Payment indication from the payment system.

**Step6:** Purchased goods or services.

### 4.4. Electronic Cash Payment Systems

Electronic cash is a store of monetary value, held in digital form, which is available for immediate exchange in transactions. Electronic cash or digital cash payment system is an anonymous token-based direct electronic macro payment system, in which the payment instrument consists of prepaid payee-independent electronic value tokens issued by trusted financial agent. The customer can use the electronic Cash payments to pay over the Internet without the involvement of banks during their payments [31].
Comparison of Current On-line Payment Technologies

In general, an electronic payment system consists of three phases and they are

- Withdrawal
- Payment
- Deposit

**Step1: Withdrawal**, The Customer [Payer] withdraws electronic coins of specific denomination from his or her on-line bank. Each of these coins consists of a serial number for unique identification and denomination value. For authentication, each coin is digitally signed by the bank.

**Step2: Payment**, The user collects the correct amount of coins and sends them across a network to make a pay. The merchant [Payee] can verify the authentication by checking the bank's signature.

**Step3: Deposit**, The payee [Merchant] sends those coins to the bank for verification to prevent a double spending. The bank prevents double spending by maintaining a database of all the spent coin serial numbers. If the coins serial numbers are not present in the bank's database then this payment is valid and the serial numbers of the coins will be entered into the Bank's database.

Electronic cash payment system is modeled after the traditional paper based payment system, so it should have the same features as the paper based payment system. Some of those features are [40].

- Anonymity
- Security
- Divisibility
- Transferability
Anonymity: As in the traditional cash payment systems, electronic cash payments are anonymous as they can't be traced back to a particular individual and it is called “unconditionally untraceable”. Here payer's [Merchant] anonymity is limited to the payee only as the financial institution can trace down the payment path, which depends on who is requesting for coins and who is depositing them. Full anonymity can be achieved by letting the financial institution to sign on the coins using blind signatures. Here the coins are blinded by the user using some blinding factor and the user sends them for getting signed by the bank authorities. The bank signed on these random looking blind coins without knowing their serial numbers and the user can now remove the blind factor and send to the merchant [payee] and the bank can't link a specific withdrawal with a specific deposit.

Security: The main security concerns of electronic cash payment system are forgery and double spending [or multiple spending]. As in the paper based payment systems, forgery or counterfeiting is the main concern in the electronic payment system. Here forged coins are created with all the genuine coin features except that without making a corresponding bank withdrawal. With strict user authentication and message integration the token forgery can be avoided.

Spending the same token over again and again is called double spending or multiple spending or repeat spending. The only method to safe guard against the double spending or multiple spending is to check the database of spent coins on line at the issuing financial institution database at the time of purchase as the issuing financial institution maintains a database of all the spent electronic coins. In an off line transaction, the identity of the user should be attached to the coin information. In a non-anonymous payment system, the user identification information can directly be attached to the coin information but in the anonymous systems, the user information will be divided and only a piece of that will be attached to the coin information[25].

Divisibility: The user needs to have correct coin denominations at the time of purchase for payment and he has to keep various denominations which lead to undesirable storage costs and coin handling problems. If the system is on line, the user can withdraw required coin denomination and the exact amount at the time of purchase. To support the off line transactions, divisible coin system is proposed. A divisible coin is an electronic coin that can be divided into smaller coin denominations and whose total value is equal to the value of the original coin.
**Transferability:** An electronic coin is transferable, if a payee [merchant] can use the received coin in the subsequent payment. A payment system is transferable if it allows at least one transfer per coin. Like in traditional cash based payment systems, transferability is well desired as it reduces the communication with the issuing bank considerably. Most of the electronic cash payment systems are not transferable as they support the single spending of coins before being returned to the banks.

There are many electronic cash payment systems available now and the most popular among them are

- Digicash
- Mondex

**Digicash:** This system was found by David Chaum and this is one of the first systems for electronic cash payments. Ecash is a fully anonymous secure electronic cash payment system developed using DigiCash. Ecash has strong security features with the implementations of both symmetric and asymmetric cryptography. Here, the customers [payer] and merchants [payees] have accounts at an Ecash Bank. The clients withdraw the coins form the Ecash bank and keep them in their Ecash wallet, software resides on their computer. The Ecash wallet is also called *cyberwallet* and these coins are used for the on-line payments [8].

**Mondex:** This system was developed by Tim Jones and Graham Higgins of the National Westminster Bank, UK. Smart card technology forms the basis for the Mondex system. The electronic cash is stored on the smart card along with personal identification number [Which is used to provide user authentication]. The electronic cash loaded in the smart card is used for the payment purpose at the POS [point of sale] with the help of specially installed Mondex automated teller machine [ATM] [8].

**4.5. Mobile Payment Systems**

With the recent developments of high-speed mobile data networks and new developments of electronic commerce, a new channel of commerce has been emerged and that is Mobile commerce. Mobile commerce is exactly the same as E-commerce except that the access mechanism is via a
mobile wireless device rather than the fixed telephone network. Mobile commerce demands more advanced and secure on-line payments over Mobile devices [Mobile Phone, Personal Digital Assistant], which support the on-line payment transactions regardless of place and time. The on-line payment methods which support above features are called mobile payment methods [24].

We define the mobile payment as wireless transaction of a monetary value form one party to another using a mobile device [Mobile phone, PDA, laptop] regardless of their geographical location [with in access limits] [13].

In addition to the possibility to pay on-line, the mobile on-line payment system offers the following ways of paying

- Person to person.
- Pay at point of sale.
- Pay on the Internet.
- Pay invoice with mobile payment system.

There are different roles such as service providing, consumer authentication, payment authorization and payment settlement which should be managed properly in the mobile payment systems. There are four actors which can take care of those roles and they are [14]

- **The consumer**: The consumer owns the mobile device and he uses it to pay for a service or product [a physical content, down loadable digital content] and he might involve in the process of initializing the mobile purchases, registering with the Payment service provider and authorizing the payments

- **The content provider** or **Merchant**: The merchant or content provider sells the products [digital content or physical content] to the consumers and he might involve in the process of forwarding purchase requests to the payment service provider, relaying authorization requests back to the consumer and the delivery of the contents.

- **Payment service provider**: The payment service provider is responsible for the payment process. He controls the flow of transaction between the mobile consumer, the content provider and the trusted third party. A payment service provider can be a network operator
or an independent payment vendor or a banker or a credit card company. He might let the consumer to be registered with him to avoid the repeated entries of payment details.

- **Trusted third party**: The trusted third party performs the authentication and authorization of the payment requests and payment settlement. A network operator, banks or credit card companies can be trusted third party.

![Mobile Payment System Transactions](image)

**Figure 4.7**: Mobile Payment System Transactions

From the figure 4.7, the content provider offers the content to the mobile users. The mobile requests for the content from the content provider. Once this content request is made, the content provider will initiate a charging session with the Payment Service Provider. The payment service provides the authorization and authentication of the mobile user to complete the payment transaction. The trusted third party performs the authentication of the transaction parties and the authorization of the payment settlement. In most of the mobile payment systems, the payment service provider itself is responsible for the authentication of the payment requests.
The generic interactive operations in a mobile payment system with three interacting parties [Mobile User, Content Provider and Payment Service Provider], which are necessary during a payment session, are explained in the following diagram [14].

![Generic operation in a mobile payment system with 3 interacting parties](image)

**Figure 4.8:** Generic operation in a mobile payment system with 3 interacting parties

**Step1, Service Registration:** The content provider registers with the payment service provider and gets a service identification number for the further operations.

**Step2, User Registration:** The mobile user registers with the payment service provider to use the services provided by content provider. The user will get an identification number after the completion of registration, which uniquely identifies the user during the on-line payment transaction.

**Step3, Requested Service:** A registered mobile user can request a service provided by a registered content provider.

**Step4, Request Charging Session:** The content provider will initiate a charging session with the payment service provider once it receives a request form the registered mobile user. The charging session is uniquely identified by a unique identification number.

**Step5, Request authorization and authentication:** The mobile user's authorization is needed before the starting of the charging session and it would be achieved by the mobile user's acceptance.
of payment agreement sent by the content provider. The mobile user's authentication can be achieved by submitting the PIN code of the mobile device.

**Step6, User Authentication:** The payment service provider confirms the authentication and authorization of the mobile user and it issues a unique session id. The content provider can start of charging the user from now on.

**Step7, Provide Content or Service:** The content provider provides the requested content of service to the mobile user.

**Step 8, Charge:** On the request of the content provider, the payment service provider settles the payment transaction between the mobile user and the content provider and informs them the results of the transaction.

Undoubtedly, the shift of physical to virtual payments has brought enormous benefits to consumers and merchants but it puts a lot of pressure on payment service providers and mobile operators to provide robust security and interoperability. The advent of mobile payments has added another layer of complexity through the use of constrained devices with different capabilities and network limitations[42].

In the mobile payment systems, Public Key Infrastructure [PKI] and Second ID Module [SIM] provide security to the user's mobile payment devices. Wireless Transport Layer Security [WTLS] provides security to the content/service providers. The emerging 3G networks can provide a secure communication medium between the mobile user and the content provider through a secure Mobile IP tunnel. This depends on these three major players [The Mobile user, the content provider and the Medium between them], the security in the mobile payments can be categorized into the layers of Application security and Channel security [41].

**Application Security:** Digital signatures provide end-to-end security form the mobile device to the back end application through the WAP gateway and WAP server. The Second ID Module [SIM] provides the application security and it supports the non-repudiation feature. SIM can even provide security in the mobile devices, which do not have the Wireless Application Protocol implemented in them. It uses SMS to achieve the intended security level[8].


**Channel Security:** Wireless Transport Layer security (WTLS) protocol provides the Channel security and it supports the privacy, data integrity and authentications in the mobile payment devices. WTLS issues certificates which authenticate the server and the client to the WAP gateway through which the mobile payment devices establish a communication[8].

One example for mobile payment systems is PayBox, which was established as a joint venture of Oracle, Compaq, Lufthansa and Deutsche Bank where Deutsche Bank owns more than 50% stake in that. Deutsche Bank deals with the client databases, clearing and settlements. This system debits the bank account to pay for a service by using a PayBox voice message to request payment confirmation and the customer uses the mobile phone to authorize the payment by entering a secret PIN code[8].
5. Micro On-line Payment Systems

5.1. Micro On-line Payment Systems
It is an on-line payment system designed to allow efficient frequent payments of small amounts, as small as a fraction of a dollar. In order to keep transaction costs very low and efficient, the communication and computational over heads are minimized here. Unlike macro on-line payments, which use expensive public key cryptography and on-line communication with the trusted third parties [most of the time], the security requirements of the micro on-line payment are relaxed by using light weight cryptographic primitives and off-line payment verifications. The security of micro on-line payment systems is not as good as that of macro on-line payment methods but if the user's micro on-line payments are tampered then the user might lose a few cents only. Here, the cost of fraud is much higher than the possible value to be gained by fraud itself. So the security in micro on-line payment methods is considered to be adequate [15].

The majority of micro on-line payment systems were designed to pay for information goods on the Internet. A network user might pay to consult an on-line database, read some financial information web-pages, listen to a song, play an on-line computer game etc. In general, the parties involved in the micro on-line payments are [18]

- Customer
- Service Provider or Vendor
- Micro on-line payment processor
From the figure 5.1, the Micro On-line payment system transactions can be explained in the following way.

**Step 1:** Customer proves his authentication and the Micro on-line payment processor issues micro payments.

**Step 2:** Customer pays the micro payments to the Service provide or vendor and gets the requested goods or services form the Service provider or Vendor.

**Step 3:** Vendor or service provider deposits Micro payments by the customer at the Micro on-line payment processor or claims money from the processed micro payments form Micro on-line payment processor.

There are 3 alternative ways to initiate payments in the micro on-line payments with 3 parties [Consumer, Micro Payment Processor, and Service Provider]. They are explained in the following diagrams.
**Alternative 1:** Consumer initiated and Consumer acknowledged payments.

**Figure 5.2:** Consumer Initiated and Consumer Acknowledged Micro On-line payments.

**Step 1:** The service provider provides the payment information to the consumer and the consumer initiates a payment.

**Step 2:** The consumer is acknowledged the payment and he sends that information further to the service provider in order to get the paid product.

**Alternative 2:** Provider initiated and Provider acknowledged payments.

**Figure 5.3:** Provider Initiated and Provider Acknowledged Micro On-line payments.

**Step 1:** The provider initiates a payment after receiving the identification information from the Consumer.

**Step 2:** The provider receives an acknowledgment and sends the received confirmation to the consumer and/or deliver the paid products.
Alternative 3: Jointly initiated and double acknowledged payments.

Figure 5.4: Jointly Initiated and Double Acknowledged Micro On-line payments.

Step 1:

Step 2: Both consumer and provider initiate the same payment and they have to provide partial payment information such that the payment system can correlate the received information to make the payment. Here, the users need to interactive with each other before the initiation in order to exchange parts of the payment information.

Step 3:

Step 4: Here, both the consumer and the provider receive acknowledgments concurrently. In general, the provider delivers the paid product after receiving the acknowledgment without any additional interaction with the consumer.

Micro on-line payment systems can be pre-paid or post-paid systems. In the pre-paid systems, the consumer transfers money to the payment system before the consumer can initiate payments and the money is stored in the form of electronic form. Here, the consumer receives the authorization of funds and he can immediately start to pay products.

In the post-paid systems, the payment system authorizes the consumer to initiate the payments before the consumer transfers money to the system. Before getting the authorization, the consumer has to present the system a reliable and valid money source to be credited over a certain time period [15].
A number of payment systems, which need to contact a trusted third party during every payment have been proposed as micro on-line payment systems, but they are infeasible to handle large number of micro on-line payments as they need to contact the trusted third party repeatedly. The micro on-line payments systems can be classified into the following 4 categories based on the cryptographic constructs used and the communication overheads [8].

- **Hash Chain based Micro On-line Payment Systems.**
- **Hash Collisions and Hash sequences based Micro On-line Payment Systems.**
- **Shared Secrete Keys based Micro On-line Payment Systems.**
- **Probability based Micro On-line Payment Systems.**

### 5.2. Hash Chain based Micro On-line Payment Systems

Hash functions are used to authenticate a payment in the micro on-line payments instead of expensive digital signatures. Here, the user computes the outcome of a one-way function \( y = f(x) \) and securely shares it with the system to which it later wants to authenticate. A hash chain of length \( n \) is constructed by applying a hash function \( n \) times to a random value labeled \( x_n \). The value \( x_n \) is called the root value of the hash chain. A hash chain derived using a hash function \( h \) recursively can be represented as:

\[
h_n(y) = h(h_{n-1}(y))
\]

\[
h_0(y) = x_n
\]

Where \( h_n(y) \) is the result of applying a hash function repeatedly \( n \) times to an original value \( y \). The final hash value, or anchor, of the hash chain after applying the hash function \( n \) times is \( x_0 = h_n(x_n) \). The hashes are numbered in increasing order from the chain anchor \( x_0 \), so that \( h(x_1) = x_0 \) and \( h(x_2) = x_1 \).

Each hash value in the chain can provide a single user authentication. The user releases \( x_1 \) for the first authentication, \( x_2 \) for the second and so on. The server only has to apply a single hash function to verify that the received value hashes to the previous value. The user only needs to store \( x_n \) from which the rest of the chain can be re-computed. The final hash \( x_0 \) of a chain may need to be securely swapped across a network. A public key digital signature can be applied to \( x_0 \) to produce a signed commitment to the hash chain. Such a user signature on the chain anchor is represented as \( \{x_0\} \text{SigUser} \). signature allows a single message to be signed once using a set of private signing
values and verified with the set of public validation values and it is having the advantage of allowing non-repudiation [proof of authentication to third parties][20].

Hash values from a user-generated hash chain can be used as authenticated payment tokens. For each micro payment, the user releases the next payment hash, the pre-image of the current value, to the vendor. Since the hash function is one-way, only the user could have generated this value, and knowledge of it can constitute proof of payment. In essence, the hash chain links the correctness of the current payment to the validity of previous payments. Each hash value is worth the same amount, which can be specified in the commitment.

This system implements the cryptographic properties of digital signature and hash chain. In this system, the Customer opens an account with the Micro on-line payment processor. The Micro on-line payment processor issues digitally signed certificates, which authorizes the customer to make payments and assures the Service Provider or Vendor that the customer's payments are redeemable. Customers create the payment hash chain in reverse order by picking the last payword $P[N]$ at random and then generate the remaining paywords [A micro payment value] by applying the formula $P[N-i] = H(P[N])$

Here $H$ is collision-resistant hash function

And $i = 1, 2, \ldots, N$.

And $P[0]$ is the root of the payword chain.

![Figure 5.5: Hash Chain Based Micro On-line Payment System Transactions.](image)
From the figure, A Hash Chain based Micro On-line Payment System Transactions are explained in the following steps.

**Step1:** The Customer registers with the Broker or trusted third party, who acts like Micro on-line payment processor. The Broker or trusted third party generates and issues a certificate to the customer and the customer is now eligible to do purchase using this Micro on-line payment system. The certificate is in the form of \( \{B,C,A_c,PK_c,E,I_c\} \text{ } SK_B \)

Where
- B: Broker or Third party identity.
- C: Customer Identity
- A_c: Customer IP-address.
- PK_c: Customer's public key.
- E: Expiration date.
- I_c: Other customer specific information.
- SK_B: Broker's signature.

**Step2:** When the customer contacts a new vendor, the customer computes a new payword chain with the root \( P[0] \) and computes his or her own commitment for that chain. That commitment is in the form of \( \{V,C_c,P[0],D,I_m\} \text{ } SK_c \)

Where
- V: Vendor's Identity.
- C_c: Client's certificate
- P[0]: Root of the payword chain.
- D: Current date
- I_m: Additional Information.
- SK_c: Customer's signature.

**Step3:** In advance of business, customer sends his or her commitment to the vendor and the vendor verifies the Client's signature and Client's certificate and the expiration date. If all the information is valid then the Vendor keeps the commitment.

**Step4:** When the Customer purchases goods or services from the Vendor then the Customer transfers the \( \{P[i], i\} \) to Vendor as its payment. So the customer sends \( \{P[1],1\}, \{P[2],2\}, \{P[3],3\} \) for 1st, 2nd and 3rd successive payment.

**Step5:** Vendor computes \( H(P[i]) \) and confirms it, if valid then keeps it.
Step6: Vendor sends the last payment information \{P[i], i\} and it's commitment to the broker or trusted third party and requests for the redemption. After verification, Broker withdraws eligible money from Customer's account and deposits it into Vendor's account.

The basic chain structure can be modified to produce tree structure, which allows multiple independent values to be authenticated through their connected branches to the authenticated root of the tree. The root node is initially authenticated by other means such as by signing it with a regular asymmetric digital signature. The basic chain structure can be modified to produce even better tree structure called PayTree, in which each leaf of the authentication tree becomes the anchor of a normal hash chain. A broker signs the root of the tree with an asymmetric digital signature. Since the anchor of each hash chain can be authenticated through the tree, the need to sign each chain individually has been removed. The contribution of PayTree is that instead of a digital signature generation per vendor for a new hash chain commitment, the computational cost has been reduced to a single signature for \(K\) vendors[18].

A broker or trusted third party aggregate micro on-line payments to many different vendors. Actual monetary value is claimed by redeeming the highest spent token along with the commitment at a broker with whom the user has an account [9]. By using a hash chain, the Computational cost of a payment is now a single hashing operation for the vendor after the Initial single digital signature verification for a new chain. If a user spends \(N\) hashes from a Chain to make \(z\) payments at the vendor then the average cost per payment is \([N \text{ hashes} + 1 \text{ Signature}] /Z\).

PayWord: PayWord is a hash chain based micro on-line payment scheme and it was designed by Ron Rivest and Adi Shamir. This scheme aims to be a fast micro on-line payment system by replacing a number of public-key operations required per payment by using hash functions. PayWord uses chains of hash values to represent user credit within the system. Each hash value called a PayWord can be sent to a merchant as a payment. A PayWord chain is vendor-specified and the user digitally signs a commitment to honor payments for that chain. Here, the broker mediates between users and vendors and maintains accounts for both. They vouch for users by issuing a PayWord certificate allowing that user to generate PayWords. They redeem spent PayWord chains from vendors, transferring the amount spent from the user's account to the vendor.
It is not necessary for both the vendor and user to have an account at the same broker. As in other micro on-line payment schemes, security is a bit relaxed for more efficiency. There is some possibility that some users might over spend and those users can be detected and removed from the on-line payment system. Since PayWord is a credit-based scheme, vendors need some assurance that users will honor their PayWord payments[17].

A PayWord certificate authorizes a user to generate PayWord chains and guarantees that a specific broker will redeem them. Brokers and vendors do not need to have PayWord certificates in the PayWord Scheme. In general, the users get PayWord certificate when they initially set up an account with a broker. Any macro payment method or credit card could be used to charge money into the account. The certificates have to be renewed every month and this limits fraud by ensuring the users who over spends will not be issued with a new certificate. A broker might maintain blacklists of certificates that have been revoked. A user's certificate would be revoked if the user's secret key are lost or stolen as this would allow others to generate PayWord chains under the user's name. The vendor can get the list of revoked certificates from a broker [18].

5.3. Hash Collisions and Hash sequences Based Micro On-line Payment Systems

In this micro on-line payment method payment coins are produced by a broker, who sells them to the users. User gives these coins to the vendors as payments. Vendor returns the coins to the broker in return for payment by other means.

![Diagram of hash collisions and hash sequences based micro on-line payment system](image)

**Figure 5.6:** Hash Collisions and Hash Sequences Based Micro On-line Payment System Transactions.
From the figure 5.6, the Hash Collisions and Hash Sequences Based Micro On-line Payment System Transactions are explained in the following way.

**Step 1:** The Users buys coins form the broker.

**Step 2:** The broker issues the coins which can be used for any vendor.

**Step 3:** The user spends the coins.

**Step 4:** The vendor sends the purchased information or goods to the user.

**Step 5:** The vendor redeem the coins with the broker at the end of the day.

Hash collisions and sequences can be used to define an electronic coin as a $k$-way hash function collision [$K$ different input values map to the same output value]. A collision occurs when two entries have the same hash. Two values $x_1, x_2$ form a two-way hash function collision if they both hash to the same value $y_1$ and it is computationally hard to generate two values to the same value.

$$H[x_1] = H[x_2] = y_1$$

A $K$-way hash function collision occurs when $K$ different input values map to the same output value of $y$

$$H[x_1] = H[x_2] = H[x_3] \ldots = H[x_k] = y$$

Broker issued payment coins as $k$-way hash function collisions and no public key cryptography is used here. Each coin is worth the same minimum value and the customer or the user stores the coins in a large scale and transmits the coins, when he makes purchases. The token are vendor independent and they can be spent at any vendor [8].

In this micro on-line payment method, the issuer creates coins and invests a large amount of computation to search for hash function collisions. Instead of using digital signatures, the collisions are used to authenticate the coins. It is efficient to verify that the coin is valid by checking that each pre-image is unique and that they all hash to the same value. The coin can easily be verified by

- Performing Hash function on each $x_i$ to obtain the same $y$ value
- Ensure that each $x$ is different. Otherwise the $x$ value could be set to be the same value and they would then map to the same $y$ value
- Verification of coin proves the authentication of the coin and the broker needs to maintain a copy of each coin already spent to check against double spending.
Coins, which are defined as \textit{k-way hash function collisions} can provide protection against forgery by imposing a coin validity criterion, in which a portion of the hash value must equal a certain bit pattern. This has the advantage of reducing the storage requirements of the bank as the non-confirming hashes can be discarded instead of storing them as candidates for possible collisions. Here the payment coins have a very short validity period and it forces the attacker to generate the coins during their short validity[15].

The definition of a coin can be modified so that the broker can prevent stolen coins being spent and he can issue user-specific coins. The user's identity \( U \) is hashed by using a second hash function \( h_2 \) to produce a group of numbers and each will be labeled \( d_i \). A coin is now a set of \( k \) pre-images \{ \( x_1, x_2, \ldots, x_k \) \} whose hash values \{\( y_1, y_2, \ldots, y_n \)\} form a sequence where the difference between each hash value links them to a specific user identity \( U \) and \( h_2[U] = \{ d_1, d_2, \ldots, d_{k-1} \} \)

\[
y_{i+1} = y_i + d_i \pmod{2^U} \quad \text{for } i = 1, 2, \ldots, k-1
\]

Coin verification will require one additional hash computation per purchase and the hash Values combine to form a hash of the user identity [18].

The customer can spend the coins at any vendor and double spending is possible as there is no checking performed to see if a coin is already spent. But when the vendor redeems the coins with the broker, the broker will detect the fraud and the users, who are repeatedly double spending can be blacklisted and expelled from the payment system.

**MicroMint**: This is a Hash Collisions and Hash sequences based micro on-line payment schemes and it was designed by Ron Rivest and Adi Shamir, who have also developed the PayWord Micro on-line payment scheme. It is based on a unique form of identified electronic cash that requires no public-key cryptographic. MicroMint coins can be spent efficiently at any vendor without the need to contact a bank or broker for the verification at the time of purchase. The security provided by this scheme is a bit less than that of the PayWord but it's an efficient micro on-line payment scheme to made payments to many different vendors. In this payment scheme, some small scale fraud is possible but large-scale fraud is designed to be computationally difficult. In this MicroMint system, coins are minted by broker, who then sells them to users. A user can speed coins at any vendor. A broker might maintain user and vendor accounts that can be settled using a macro payment
scheme[15].

5.4. Shared Secrete Keys Based Micro On-line Payment Systems

In this micro on-line payment schemes, sharing the keys between the parties concerned eliminate the use of computationally expensive asymmetric cryptography. By using the Message Authentication Code [MAC], shared secrete keys can be used to provide authentication and integration. Here, a secrete key K is appended to the message M and a hash function applied to the combined value and the symmetric encryption using the shared key will provide message secrecy. Instead of a full encryption, a one-time pad can also provide secrecy. One-time pad can be generated by choosing a random number N and it would be hashed with the secrete key K and XOR'ed with the message to hide. Now, XOR'ed message is sent with N and the user needs the secrete key K to recover M.

Public key cryptography of out-of-band communication is used to solve the key distribution problem as the symmetric keys have the problem of how initially to swap the secrete value for a new relationship. Here, each key need to be refreshed periodically to prevent cryptanalysis and to limit the time frame of a brute force attacks[8].

Millicent: This is one of the first micro on-line payment system designed on the basis of Shared Secrete Keys scheme and it uses a broker to aggregate user micro on-line payments made to many vendors. It uses vendor-broker and user-vendor shared secrets. Here, vendor issues value to users in the form of an authenticated message, which is called scrip, which specifies the value a user, has at that specific vendor. To ensure that scrip is genuine, the vendor uses a vendor secrete in a keyed hash of the scrip to produce a Message Authentication Code [MAC].The MAC prevents the scrip being altered or forged. The vendor can verify the scrip by re-computing the MAC. A serial number is placed in each scrip along with the value and other fields to prevent double spending. Scrips can be verified locally as they are vendor specific. A broker sells the vendor scrips to customers and the vendor shares its MAC vendor secretes with the broker to allow it to generate vendor scrip. To avoid any fraud by eavesdroppers, the customer and the vendor share the customer secret, which is given to the customer by the broker upon new vendor scrip purchase [48].
The system is primed by making a macro on-line payment to the broker to obtain value in the form of broker scrip. Vendor scrip is then purchased using this broker scrip. Since the value is vendor specific, the broker will be contacted on-line to buy vendor scrip for a newly encountered vendor. All the further purchases with that scrip are off-line and the user must trust the vendor and broker as the user can't verify the scrip message independently. The Millicent micro on-line payment scheme can be explained by the following figure[56].

![Figure 5.7: Shared Secrete Keys Based Micro On-line Payment System Transactions.](image)

From the figure 5.7, the Shared Secrete Keys based Micro on-line Payment System Transactions can be explained in the following steps
Step1: The Customer buys *vendor scrip* form the broker.
Step2: Customer buys information or product with *vendor scrip*.
Step3: Broker buys or produces large chunks of *vendor scrip* for licensed vendor.

**5.5. Probability based micro on-line payment schemes.**
This scheme supports to minimize the number of transactions the must be performed for each and every payment. This is a deferent approach than some other micro on-line payments as they need
each and every payment is usually processed by the vendor and later verified and redeemed at the trusted third party. Here, probability theory can be applied so that there is a specified chance that transaction will be performed and it reduces the number of transactions must be performed for each and every transaction[6].

Here, the micro on-line payment cost has been eliminated for most of the transactions with the introduction of cost of fairly predicting a random event with known probability. Probability techniques have also been applied to the creation of digital signatures. It can solve the difficulty of factoring and it can be modified to allow more compact signatures to make no use of memory between signatures other than for the public and secret keys. The factoring-based version of this scheme is more practical and it can well safeguard the security properties of the payment system. The probability signatures based on efficient public key algorithms can offer a significant performance improvement with little increased risk of forged signatures [8].

**Bets using coin flips:** Wheeler, Proposed this Probability based micro on-line payment scheme, in which, for each transaction the payer makes a bet with the payee. If the payee wins the bet then an actual micro payment is made to the payee by the payer otherwise no payment is made. The transaction value is set by fixing the probability of the payee winning the bet to specific value[8].

**Hash chain lottery tickets:** Rivest, proposed this probability based micro on-line payment scheme. Here each payment is probabilistic as each ticket has a known probability of winning a specified amount. The user will only make an actual payment for winning tickets. In this scheme, the overhead of processing every micro payment at the bank is reduced to only processing winning payments[8].

The efficiency of probabilistic payment is similar to other micro on-line payment schemes for both the user and the vendor. Due to the probabilities there will be a variability of the amount paid and an unlucky user will end up paying more than expected. The main advantage of this scheme is that the bank needs to process only the winning micro payments and it supports more anonymity as the bank will not see every transaction[18].
6. Comparison of Current On-line Payment Systems

The comparison of current on-line payment systems, is based on the following factors, which have been briefly discussed in the chapter 3 [Classification and Requirements of On-line Payment Technologies].

- Security issues
- Usability issues
- Reliability Issues
- Anonymity/Privacy Issues
- Scalability Issues
- Monetary Value
- Customer Acceptance

6.1. Analysis of Macro On-line Payment Systems

Macro On-line payment systems allow secure on-line payments ranging from one US dollar to several thousand US dollars. These on-line payment systems are modeled on real world payment instruments and transfer larger sums of money for each transaction. So, usually the security requirements are more rigorous. These transactional over heads and heavy usage of computationally expensive cryptographic operations prevent these payment systems to be used for the payment of small amounts [amounts ranging from a fraction of a US Dollar to one US dollar].

Security of Macro On-line Payments

Macro payment schemes normally use public key cryptography for authentication purpose. This is used to prevent forgery. Macro payment schemes use encryption to preserve privacy of the data and these payment schemes use on-line broker activities to detect double spending prior to the acceptance of a payment by the vendor.

Draw backs of Macro On-line payments

- Security Issues
  - The main problem with the macro on-line payment is the security of the system. The large
number of payments handled by the system, the more attractive it would be for hackers to attack the system.

- It also faces problems in Handling of credit risks, currency risks, money float, and liquidity of the system etc.

**Usability Issues**

- Macro payment imposes a minimum cost per transaction and It also raises the cost of the transaction as the bank is faced with the real cost of authorizing each transaction. As a result, the macro payment systems are not suitable for low value payment transactions.
- It uses computationally expensive cryptographic operations, such as public key cryptography. It prevents them for using it for payment of small amounts [few cents].

### 6.1.1. Analysis of Credit Card Based Payment systems

Despite the increased risk, the absence of commonly accepted network payment schemes in a period when the Internet was rapidly expanding and which meant that many people resorted to this method of effective payment.

**Advantages of Credit Card Based Payment System**

**Customer Acceptance**

- At present, credit card payment systems offer the most practical and popular payment methods for on-line payments over the counter electronic payments methods.

**Security Issues**

- Credit Card payments reduce the risk and costs associated with handling cash and checks.
- Credit cards for on line payments have a large user-base and benefit from familiarity and simplicity of use and also allow international payments. Security is being addressed via new modified credit card payment solutions.
- Another advantage of the secure credit card model is that the user needs not be registered to the payment service, only the transportation of the credit card number is needed for instance in encrypted form.

**Reliability Issues**

- One of the main advantages of the credit-debit model is the audit ability of the transactions which is certainly a desired feature from the viewpoint of the merchants and banks. The
transactions can always be traced so that it can be determined, "who paid, how much, for what, with which instrument and when".

**Usability Issues**

- Another important advantage to be noted is that the credit card organizations already have business experience in managing similar systems and many of them have very large customer bases already.
- Portable
- Possible reductions in mail-handling delays and costs with fewer errors and lost transactions.
- Faster fund deposit and availability at the bank, usually less than 24 hours.
- Improved turnaround time to customers and increased opportunity for automation of accounting, banking and reconciliation processes.
- Opportunity for decreased costs though transactional volume available with centralized shared services.
- As customers shift to the Internet for services, some savings may be seen in reduced pressures on over-the-counter, mail, and phone customer-support services.
- Increased customer access (24x7 service availability) and for automated systems, reduced transaction data-entry time.

**Drawbacks of Credit Card Based payment System**

**Security Issues**

- On-line payments with credit cards can be risky. Some customers may find that, when the credit card statement comes, many entries have been made without their consent or even their knowledge at all.
- There is an awareness of fraud and other security issues concerning e-payments by credit cards. The information may be intercepted or altered during transmission. The information may be stored on vendors servers and they may fall victims to hackers who may later sell the information or use the information to make illegal purchases. Dishonest vendors may sell the information. All these threats expose credit card holders to a significant financial
Comparison of Current On-line Payment Technologies

risk. Credit card holders are not informed of these losses until their monthly statements arrive.

- Normally, cardholders are asked to supply additional information, such as their name and address, that can be used to verify their identity. If goods that require physical delivery are being ordered, they must be dispatched to the address associated with the card. This gives limited protection against bogus orders. Since there is no card holder signature involved, the processing rules allow the buyer to opt out of any transaction if they claim that they did not agree to the purchase. Clearly, this increases the risk borne by merchants.

- Using credit cards to make payments across computer networks has some security risks. Attackers eavesdropping on network traffic may intercept messages and capture credit card details as well as any associated verification information (name, address etc). Because of the distinctive structure of credit card numbers, with their inbuilt check digits, programs can be written to scan a data stream for occurrences of such patterns. The data stream could be either an intercepted transmission, a file on disk, reclaimed disk space on a shared system, or even the stream of keystrokes produced by someone typing at their workstation. If merchants are processing orders electronically, then fraudsters can generate vast numbers of orders before the fraud is detected.

- On-line credit cards have a high fraud risk and the estimated fraudulent on-line credit card payment will cause a loss of billions of dollars and it is showing the growing up trends. Because of the high transaction costs and other security risks, a number of merchants searching for other alternative payment methods and who prefers to use card payments are slowly declining.

Anonymity/Privacy Issues

- One of the drawbacks of the systems include the lack of anonymity and the fact that liquidity is dependent on the merchant’s bank.

- Paying by credit cards reveals payers identity to providers and vendors. Some users do not want other parties to know which items they have bought or which web sites they have visited. The trails usually show themselves up on the monthly statements.

Usability Issues

- Credit card payments do not include any measure to limit the spending on each vendor.
Spending limit setting can be built into the models to prevent bad vendors from repaying a transaction to get paid twice.

- Credit card payments do not include setting of daily limit. The only limit is the card holder's remaining credit line. The suggested models can be embedded with the daily budget setting to prevent inadvertent overspending.

- One of major disadvantages of credit card purchases is their high cost, both to the customer and merchant. This makes them unsuitable for low-value purchases.

- The credit card payments have a minimum threshold value and a lower value payment can't be made because of high transaction costs and this threshold has no fixed value.

- These cards are not available for everybody [young people without solid income or solid financial background].

- Cost will have a major bearing and credit card systems do not fare well on that score.

- New or increased costs associated with transaction charges, merchant fees, multiple decentralized applications and processes.

- Some initial costs to fund investment in technology, controls, require new skill sets, business processes and controls to mitigate exposures to new risks.

**Scalability Issues**

- One size does not fit all government agencies.

**Other Issues**

- Legislative issues and Credit card transactions may violate public-funds-handling laws.

### 6.1.2. Analysis of Debit Card Based Payment Systems

**Advantages of Debit Card Based Payment System**

**Usability Issues**

- Obtaining a debit card is often easier than obtaining a credit card, creating more potential users.

- Returning goods or canceling services purchased with a debit card is treated as if the purchase were made with cash or check.

- Opportunity for automation of accounting, banking and reconciliation processes.

- For automated systems, reduced transaction data-entry time.

- Impetus for various business re-engineering opportunities.
Comparison of Current On-line Payment Technologies

Security Issues

- Reduced risk and costs associated with handling checks and collection activities.
- Fewer errors and fewer lost transactions.

Drawbacks of Debit Card Based Payment System

Security Issues

- Debit card payments are directly withdrawn from the bank account and not from an intermediary account in contrast to credit cards. This can make it difficult for consumers to handle a dispute/charge back, since there is typically no extra protection of the funds in a debit account. Once the funds have been withdrawn, they are harder to refund than with a credit card.

6.1.3. Analysis of Stored Value Payment Systems

Security of Stored Value Payment Systems

A stored-value card maintains a temporary account balance, rather than actual electronic tokens, on a smart card. The card securely holds trusted bank keys, which are used to digitally sign messages passing between cards. Value transfer occurs when the payer’s card sends a signed payment instruction to the payee card or terminal. Having received an acknowledgment, the payer card will decrement its balance counter by the specified amount.

Advantages of Stored Value Payment Systems

Usability Issues

- Flexibility in adding applications giving extra value to consumers.
- Over the counter and Internet transactions possible.
- Low costs and ideal for low value transactions.
- Can be used for on line and off line transactions.
- Immediate transfer of funds.
- Cash balances remain high because of unspent balances in the cards.
- Transactions are easily processed via existing POS equipment.
- Mobile source of money.
- Transaction times are typically faster than for credit card or debit card payments.
- Increased consumer convenience.
**Security Issues**

- Secure with the use of passwords/pins.
- Risk is limited to the value of the cash sent on the network.
- Electronic transactions are faster and more accurate than counting and collecting cash or manually processing paper checks.

**Scalability Issues**

- No new or expensive investment in hardware is required.
- Each transaction is tracked electronically on a central database.

**Drawbacks of Stored Value Payment Systems**

**Scalability and Usability Issues**

- Hardware specifications pose a problem.
- Does not allow micro merchants.
- Uses proprietary currencies thus depend on issuing companies to honor their individual cash.

6.1.4. Analysis of Electronic Account Transfer Payment Systems

**Advantages of Electronic Account Transfer Payment Systems**

**Usability Issues**

- Electronic Account transfer systems have a large user base and established network, and banks have well-established procedures and security systems for on line banking.

**Drawbacks of Electronic Account Transfer Payment Systems**

**Usability Issues**

- International payments and micro payments remain challenges and the relatively low offer of e-banking for on line purchase in several countries suggests that these systems still need further development to become widespread payment options.

6.1.5. Analysis of Electronic Cash Payment Systems

**Security of Electronic Cash Payment Systems**

Electronic Cash are bit strings and that can be copied as many times as desired. In such cases, the service of protection against double spending can help. This service can be based on conditional anonymity, the condition being that if a customer is honest and spends a coin only once, his identity
cannot be discerned. However, if he does try to double-spend, he can be identified and eventually made responsible. Banks can try to prevent multiple spending by keeping a database of spent electronic tokens or coins which is checked before completing a payment. This method is useful when the transaction is done on-line, here the merchant verifies the validity of the payment before delivering merchandise. In an off-line setting, the merchant deposits the payment after merchandise has been delivered and the best thing one can do is to detect multiple spending and identify the guilty user so they can be punished. An obvious way to protect Electronic Cash from being stolen through eavesdropping is to use encryption. To ensure that a serial number is not spent twice, the minting bank must record every Electronic coin that is deposited back to that bank. Clearly, the size of the Electronic cash database could become very large and unmanageable. By using expiry dates with coins, the serial numbers of those coins can be removed after the expiry date. Coins that have expired will not be accepted as legal tender. The bank host machine needs to have an internal scalable structure to cope with the size of the database. To further handle the problem of scalability, multiple banks, each minting and managing their own currency with interbank clearing, could be used.

**Advantages of Electronic Cash Payment Systems**

**Security Issues**
- Secure with the use of encryption.
- Reduced fraud.
- Reduced check inventory security risks, reduced risk of theft, loss or damage to checks in the postal system.

**Anonymity/Privacy Issues**
- An advantage of the electronic currency model is that the payments offer (possibly full) anonymity to the user, which may encourage some potential users to start using the payment mechanism.
- Eliminates the third party.

**Usability Issues**
- Electronic cash offers the greatest possibilities for electronic trading.
- Allows micro-merchant payments which are perfect for low value transactions
- Once received, it has value immediately.
Comparison of Current On-line Payment Technologies

- Reduced cash handling, check handling, or credit card processing.
- Faster value into the bank and elimination of collection risks, checks and credit cards can be rejected or “bounced.”
- Reduced debt-collection efforts, check-processing costs, postage fees, postage-paid and return envelopes.
- Reduced efforts to replace lost or destroyed payments, transfers to unclaimed property.

**Scalability Issues**
- Software solution. No extra hardware required

**Drawbacks of Electronic Cash Payment Systems**

**Scalability Issues**
- The servers that handle payment transactions need to collect data from the past transactions to prevent the double spending of the tokens. This leads to the problem of large databases in these payment systems.
- There are many flaws to be addressed. The lack of open standards between systems is one of the major obstacles, but portability and permitting macro-payments also have to be worked out. Moreover, in micro payment systems applying this payment model the number of transactions to be logged may be huge (certainly larger than in credit card systems), thus requiring substantial storage and processing capabilities from the servers that handle the transactions. These requirements also make the tracing of the payments harder from the viewpoints of the merchant and bank.
- Uses proprietary currencies thus depend on issuing companies to honor their internet cash. Consumers are slow to trust such a system.
- Tied to specific machines (wallet on hard drive) and not portable.

**Anonymity/Privacy Issues**
- These payment system lacks some of the properties of physical cash such as anonymity, and transferability.

**Usability Issues**
- Obvious shortcomings include the fact that the user must have the exact change to be able to make the payment and that the bank must be contacted on-line during each purchase to prevent double spending.
Comparison of Current On-line Payment Technologies

- If there are fees associated with the Electronic cash system, every government will have to determine who absorbs those fees. If a government doesn’t know who pays whom, how can it collect an income tax? If the ownership of financial assets is indeterminate, what happens to taxes on financial assets?

- Lack of Standards and protocols, One of the primary reasons for the lack of development in the electronic cash arena. With each new form of digital cash, there seems to be a slightly different set of standards and protocols. Keep in mind that, in order to use electronic cash, both the payer and the payee must be previously set up to use the specified form of electronic cash. At this point, no one form of electronic cash has become a dominant player in the industry. Therefore, we see different types of electronic cash becoming localized in different geographic areas.

- Lack of Customer experience. Another common problem with electronic cash is the lack of hands-on experience in dealing with it. Few people have actually used electronic cash. The lack of experience primarily ties to the fact that electronic cash has not become a dominant player in the market.

6.1.6. Analysis of Electronic Check Payment Systems

Advantages of Electronic Check Payment Systems

Usability Issues

- Because the process is familiar to users, electronic checks may act as a stepping stone to the introduction of more dynamic payment methods.

- Third party authenticates users.

- Basic system in place already and the existing system is used and trusted by consumers.

- Just using the Internet as a method of delivery and migration form paper check to electronic check is not huge.

Security Issues

- Secure with the use of encryption.

- Risk is limited to the value of the check and if cashed without proper ID, bank identifies the customer.
Comparison of Current On-line Payment Technologies

**Drawbacks of Electronic Check Payment Systems**

**Usability Issues**
- Costs are too high for low value transactions
- Does not allow micro-merchants.
- Only sender's bank can issue value for the check.
- Slow method, no immediate transfer of funds.
- No immediate confirmation
- No guarantee of payment upon receiving a check.

**Anonymity/Privacy and Portability Issues**
- No anonymity.
- Not portable.

6.1.7. Analysis of Mobile Payment Systems

**Security of Mobile payment Systems**

Security characteristics differ across services. As a general aspect for mobile phones, they offer additional possibilities for customer authentication, specifically SIM and PIN. For specialized payment services, security is assured via multiple measures; a personal PIN, the phone number and the mobile phone (e.g., SIM card) itself. All of this is necessary for payment. Furthermore, the connection between the handset and the base transceiver station (BTS) is encrypted.

**Advantages of mobile payments**

**Usability Issues**
- On-line Payments using mobile telephone are currently considered highly promising because customers will be able to pay for products anywhere and anytime.
- Mobile devices have the potential to facilitate cross-border payments for future payment schemes.
- Mobile payments provide additional authentication possibilities without the need for additional hardware, this gives them some advantage in developing secure and convenient payment systems.
Security Issues

- The mobile payments service providers will offer the necessary trust that customers require to make the payments and guarantee the payments for merchants.

- Using mobile devices for payments has major potential due to the very large user base and familiarity with mobile phones and billing systems. Costs are potentially low (payments added onto an established payment system), security can be established with extra pin-numbers, and micro payments can simply be aggregated into overall payments.

Drawbacks of Electronic Check Payment System

Security Issues

- The issues of payment authorization, common standards and physical security of the device need to be solved.

Interoperability Issues

Challenges exist in relation to international payments and there is the question to what extent new intermediaries (mobile operators) can act as financial intermediaries.

6.2. Analysis of Micro On-line Payment Systems

Micro On-line payment methods support frequent transfer of very small amounts as small as a fraction of dollar[even less than a cent]. Because of the small amounts involved, higher efficiency can be achieved by slightly relaxing the security mechanism. In order to keep transaction costs very low and efficient, the communication and computational over heads are minimized here.

Security of Micro Payment Systems

Well-designed micro payment system implementations allow exact replay of the messages to the same origin within a few minutes interval by identifying the double spending attempts. Some micro payment systems allow the brokers of the system to accept low-level of complaints automatically and without any questions. The complaints are logged and pattern of abuses can be used to identify the culprit - this way a suspected fraud can be traced quite easily. It is, however, absolutely impossible and unprofitable to investigate every complaint due to nature of the micro payments. The disappearing of a single micro payment is not dangerous or fatal for the security of the system or the user. The micro payment systems need not be as secure as for instance the credit card
Comparison of Current On-line Payment Technologies

systems, since the potential loss of a single payment is not financially disastrous for any party of the transaction because of the very low value of the payments. Moreover, the data of low-value transactions is probably not valuable to the attacker as such.

**Advantages of Micro on-line payment Systems**

**Usability Issues**

- Micro payment systems are usually meant for buying the low-value services only in pay-per-visited-link-style in the Internet. Since the services and goods that can be purchased in the Web are intangible, micro payment systems have been seen as the solution to the growing demand of better electronic payment systems.

- Micro payment systems allow the user to purchase goods on the Internet without having to comply to restrictions in respect of their physical presence, the purchasing time and the paying instrument.

- Micro payments provide users with more options for on-line payments. Web servers have different backgrounds and frames of mind. The web site that provides more options has a higher chance of gaining a wider customer base.

- Micro Payments are convenient on-line payments for people with no credit cards and they are an alternative for people who are not willing to fill in credit card numbers on web pages.

- Micro payments are potential and efficient alternatives when credit card systems are unable to transfer small amount of money.

- Aggregation considered to be the key for the micro payment system. Small payments are aggregated until they are settled in a macro payments

- Micro payments support small value payments for products with a minimal delay and in exchange the products are instantly delivered.

**Security Issues**

- Micro payment systems are payment systems which support low value payments at a low transaction costs. Unlike macro on-line payments, which use expensive public key cryptography and on-line communication with the trusted third parties [most of the time], the security requirements of the micro on-line payment are relaxed by using light weight
cryptographic primitives and off-line payment verifications. So the transactional overheads are minimal.

- Other considerable benefits of Macro payments over credit card payments are: The risk and the scale of loss or fraud for consumers and providers is small and these systems do not need features like high security, non-repudiation, Money-back guarantee etc.

- Secure with the use of encryption.

- Verification of user is not important as there is immediate transfer of funds.

- Risk is limited to the value of the cash sent on the network and one of the strongest points of micro payments is that the overhead to re-use or forge the coins are far too high to be of any benefit.

**Drawbacks of Micro On-line Payment System**

**Usability and Interoperability Issues**

- Micro-payment system's inability to allow macro-payments and the fact that they are vendor specific suggests they will not provide the ultimate solution, as they would be administratively difficult to regulate and would not allow experimentation on the part of customers.

- The area of micro payments has seen a range of developments but none has achieved sufficient reach and practicality to substitute the more prevalent subscription systems as the payment option.

- Not mobile.

- Uses proprietary currencies thus depend on issuing companies to honor their inter net cash.

- One of the reasons that micro payments are not widely used is that most systems require that consumers download the plug-in for their browsers. If micro payment systems were all following the same standards (like credit cards do), consumers would have been more willing to have the systems. But now the micro payment systems on one web site can be different from those of other web sites. In this case, it means the consumer needs several plug-ins or client software packages. These added troubles discourage the growth of micro payments.


**Security Issues**

- The security of micro on-line payment systems is not as good as that of macro on-line payment methods.
- The security of the hash collision and hash sequence schemes rely on the premise that very large initial computations performed by the broker cannot be performed by a determined adversary. This will require a large investment in specialized hardware, which will need to be regularly upgraded as cryptographic processors become faster and more widespread. Also, by generating coins in advance, a surplus of coins will have to be created to ensure that the maximum possible user requirements are met. Identified coins and hidden predicates are used to detect and limit large-scale fraud by an adversary with equal computational ability.
- In shared Secret key Micro Payments, While symmetric keys are more efficient, there is the problem of how initially to swap the secret value for a new relationship. Public key cryptography or out-of-band communications is used to solve this key distribution problem. In a large system, the number of shared secrets that each entity must securely keep can become unwieldy. In addition, each key needs to be refreshed periodically to prevent cryptanalysis and to limit the time frame of a brute force attack.
- There are many systems supporting micro payments in the definition of handling of the payments bellow few cents but not designed for small micro payments. Even though it is theoretically possible to make a true payment there may be problem increasingly with the smallness of the payments. The problem can be described in 2 ways
  1) The cost of transaction will at some point be higher than the amount transferred.
  2) The time and the effort for the consumer to pay. If transferred into a monetary value, will at some price level exceed the amount to be paid. It means the cost of payment is some times higher than the amount paid.

**Reliability Issues**

- A serious drawback of micro payment consolidation is the unlimited customer credit, which can only be halted by revoking the user’s certificate. This is a consequence of replacing a central broker, who controls user credit and payment aggregation, with direct aggregation between distributed vendors.
6.3. Comparison of Macro and Micro payment Systems

The Comparison of macro and micro payment systems is more based on security and usability requirements. While macro payment schemes are more concerned with the authenticity and privacy of data and therefore need demanding encryption algorithms and on-line processing, micro payment schemes aim at providing a decent level of security for transactions with more economical time and storage requirement.

- Of the two types of payments, macro on-line payments transfers payments ranging from one US dollar to several thousand US dollars of money for each transaction, so usually the security requirement is more rigorous.

Micro On-line payment methods support frequent transfer of very small amounts as small as a fraction of dollar (even less than a cent). Because of the small amounts involved, higher efficiency can be achieved by slightly relaxing the security mechanism. In order to keep transaction costs very low and efficient, the communication and computational overheads are minimized here.

- Macro payment schemes normally use public key cryptography for authentication purpose. This is used to prevent forgery. Macro payment schemes use encryption to preserve privacy of the data and these payment schemes use on-line broker activities to detect double spending prior to the acceptance of a payment by the vendor.

The security of micro payment schemes is apparently not as good as that of macro payment schemes. However, if a micro payment scheme is designed so that a customer only loses a few cents when his transaction is tampered with, and the cost of counterfeiting a coin is either computation- or policy-wise higher than the value of the coin, then the security is considered to be adequate. Compared with macro payment schemes, the computational times of micro payment schemes are less because they use one-way, collision resistant hashing extensively and minimize the use of expensive public key cryptography.

- Micro payments are potential and efficient alternatives when Macro payment systems (especially credit card systems) are unable to transfer small amount of money and aggregation considered to be the key for the micro payment system. Small payments are aggregated until they are settled in a macro payments.
Other considerable benefits of Micro payments over Macro payments (especially credit card payments) are: The risk and the scale of loss or fraud for consumers and providers is small and these systems do not need features like high security, non-repudiation, Money-back guarantee, etc.

Macro on-line payments use on-line broker activities to detect double spending prior to the acceptance of a payment by the vendor. Micro payment schemes generally avoid on-line verification by the broker. This saves the broker on-line processing time and on-line storage requirements. In addition, micro payment protocols generally keep the customer-vendor relationship transient to avoid both the necessity of setting up account-based systems on vendor sites and a potential performance bottleneck for one-time or infrequent customer-vendor interactions.

The transactional overheads and heavy usage of computationally expensive cryptographic operations prevent macro payment systems to be used for the payment of small amounts (amounts ranging from a fraction of a US Dollar to one US dollar). The computational and storage costs of micro payment schemes are suitable for small payments (e.g. purchasing a web page). Micro payments support small value payments for products with a minimal delay and in exchange the products are instantly delivered.

In Macro On-line Payments, security threats or dishonest practices can lead to a significant financial risks [can be billions of dollars]. In Micro On-line Payments, Risk is limited to the value of the cash [a fraction of Dollar] sent on the network and one of the strongest points of micro payments is that the overhead to re-use or forge the coins are far too high to be of any benefit.

Some Macro Payment Systems [especially Credit Card Based Payment System] ask the users to enter the payment details and supply additional information, such as their name and address, that can be used to verify their identity. Some users do not want to provide all these details through the Internet and do not want others to know which items they have bought or which web sites they have visited.

Micro Payments are convenient on-line payments for people with no credit cards and they are an alternative for people who are not willing to fill in credit card numbers on web pages.
Some of the Macro Payment Systems [Credit Card Based Payments etc] have a large user-base because of their familiarity and simplicity of use. They also allow international payments. These payment systems offer the most practical payment method and have become the most popular payment methods for Internet and over the counter electronic payments. Micro-payment system's inability to allow macro-payments and the fact that they are vendor specific suggests they will not provide the ultimate solution, as they would be administratively difficult to regulate and would not allow customers experimentation.
7. Conclusion

A central challenge for on-line payment methods is to provide authentication mechanisms that allow both secure payments and convenience of the transaction process. Although there is a large range of on-line payment systems, credit cards for payment and SSL for security are dominant. However, there are significant differences across countries, and other payment methods are of importance in some countries. Innovative new payment options have not often succeeded in replacing established ones.

At present, credit card payment systems offer most practical on-line payment method and have become most acceptable payment methods for Internet over all the on-line payment systems despite of their disadvantages of high cost and unsuitable for low-value purchases. Credit cards for on-line payments have a large user-base and benefit from familiarity and simplicity of use and also allow international payments. Security is being addressed via new modified credit card payment solutions.

Debit cards are an alternative payment system, especially where they previously enjoyed popularity for off-line payments and where they enjoy a broader user-base on the consumer side. However, they cannot be used in international payments in the majority of cases. Further, Debit cards are not currently suitable for micro payments.

Electronic checks do not seem to offer a solution to stakeholder desires for cashless payments. Again high cost is a major drawback and it is not facilitating low value payments, no anonymity, not being portable, no confirmation, slow transaction speed, and liquidity problems. However, because the process is familiar to users, electronic checks may act as a stepping stone to the introduction of more dynamic payment methods.

Electronic cash offers the greatest possibilities for electronic trading but has many flaws to be addressed. The lack of open standards between systems is one of the major obstacles, but portability
and permitting micro-payments also have to be worked out.

Electronic Account transfer systems have a large user base and established networks, and banks have well-established procedures and security systems for on line banking. International payments and micro payments remain challenges and the relatively low offer of e-banking for on line purchase in several countries suggests that these systems still need further development to become widespread payment options.

Mobile payment system has major potential due to the very large user base and familiarity with mobile phones and billing systems. Costs are potentially low (payments added onto an established payment system), security can be established with extra personal pin-numbers, and micro payments can simply be aggregated into overall payments. There are some challenges that exist in relation to international payments and there is the question to what extent new intermediaries (mobile operators) can act as financial intermediaries.

Micro-payment systems may play a role in advancing electronic payments but their inability to allow macro-payments and the fact that they are vendor specific suggests they will not provide the ultimate solution, as they would be administratively difficult to regulate and would not allow experimentation on the part of customers. The area of micro payments has seen a range of developments but none has achieved sufficient reach and practicality to substitute the more prevalent subscription systems as the payment option.

It can be extracted from the study that credit card based payment systems are the most widely used means of conducting on-line payments. It is evident that credit card based payment systems satisfy stakeholder requirements the best, as they offer most flexible payment options and these concepts are not alien to users. Other systems lack the flexibility to allow on-line and off-line payments, as most are specifically designed for Internet use. It can be extracted from the study that users want more simplified, convenient and secure on-line payment systems. Thus developers will have the task to incorporate all types of payment into one system, which is available for everybody’s use.
References

Books and Articles
Comparison of Current On-line Payment Technologies


Comparison of Current On-line Payment Technologies


Web References

[34] Public Key Infrastructure Overview


[36] Electronic Payment Premier

[37] Credit Card security and E-payment

[38] Stored Value Cards: An alternative for the Unbanked?

[39] The Electronic Check Architecture

[40] Achieving Electronic Privacy

[41] Mobile Payments
www.nrothstream.se [2006-05-28].

[42] Mobile payments world

Http://web.mit.edu/kerberos [2006-04-21].
[44] RSA Data Securities

[45] Design Goals of Kerberos

[46] How Credit cards work
http://www.find.co.uk/credit_cards_centre/ [2006-05-10].

http://www.bis.org/publ/cpss38.pdf [2006-04-05].


[49] Risk Management for Electronic Banking and Electronic Money Activities
http://www.bis.org/publ/bcbs35.pdf [2006-05-20].

[50] Mobile Commerce

[51] Micro Payments Overview
http://www.w3.org/ECommerce/Micropayments/[2006-06-07].

[52] Understanding Public Key Infrastructure, RSA Technologies
www.comms.scitech.susx.ac.uk/fft/crypto/understanding_pki.pdf [2006-04-10].

[53] PKI-forum

[54] RSA Security
www.rsasecurity.com[2006-04-18].

[55] VeriSign

[56] MilliCent
www.millicent.com[2006-06-14].

[57] The Secure Sockets Layer Protocol(SSL)

[58] Understand the Difference between Public Key and Symmetric Key
# Appendix & Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH</td>
<td>Account Clearing House</td>
</tr>
<tr>
<td>ATM</td>
<td>Automatic Transaction Machine</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Consumer.</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to Business</td>
</tr>
<tr>
<td>BTS</td>
<td>Base Transceiver Station</td>
</tr>
<tr>
<td>C2C</td>
<td>Consumer to Consumer</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CF</td>
<td>Cipher Feedback</td>
</tr>
<tr>
<td>CRL</td>
<td>Certification Revocation List</td>
</tr>
<tr>
<td>Card</td>
<td>Credit Card or Debit Card.</td>
</tr>
<tr>
<td>Credit</td>
<td>To increase the balance</td>
</tr>
<tr>
<td>Debit</td>
<td>To decrease the balance</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard.</td>
</tr>
<tr>
<td>Digital Cash</td>
<td>Cash stored in the digital form</td>
</tr>
<tr>
<td>EFT</td>
<td>Electronic Fund Transfer</td>
</tr>
<tr>
<td>FSML</td>
<td>Financial Service Markup Language</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest5</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>P2P</td>
<td>Person to Person</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>RSA</td>
<td>Asymmetric Encryption Algorithm</td>
</tr>
<tr>
<td>SIM</td>
<td>Second ID Module</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Smart Card</td>
<td>Single chip computer device to store data in a secure way.</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Protocol</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
<tr>
<td>WML</td>
<td>Wireless Markup Language</td>
</tr>
<tr>
<td>WTLS</td>
<td>Wireless Transport Layer Security</td>
</tr>
</tbody>
</table>
På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/

In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

© Ravi Kumar Mandadi