SRINIVAS UNIVERSITY

Mangalore-575001, Karnataka (India)

Research Centre for E-Com Challenges to Security Issues

Ms. Shilpa. K.
Research Scholar and Lecturer in Srinivas University
Email id: shilpakudroli@gmail.com

E-commerce is the process of buying and selling of various products and services by businesses through the internet. E-commerce is the web to conduct business but when we concentrate on commercial deals among organizations and individuals demanding selective information systems under the guarantee of the firm it accepts the form of e-business. It encompasses the entire scope of online product and service sales from start to finish. E-commerce tools include computer platforms, applications, solutions, servers and various software formats manufactured by e-commerce service providers and purchased by merchants to increase online sales.

Without proper security measures in place, e business are at risk of losing customer's data and revenue. Security risks associated with e-commerce can be as a result of human error, an accident or unauthorized access to systems. Security issues in e-commerce such as integrity, authentication and non-repudiation must be dealt with effectively for any online business to be successful. To solve the security issues in e-commerce, merchants and payment companies should collaboratively come up with effective solutions.

SECURITY ISSUES IN E-COMMERCE:

E-commerce security is nothing but preventing loss and protecting the areas financially and informational from unauthorized access, use or destruction. Due the rapid developments in science and technology, risks involved in use of technology and the security measures to avoid the organizational and individual losses are changing day to day. There are two types of important cryptography we follow for secured E-commerce transactions.

Symmetric (private-key) cryptography: This is an encryption system in which sender and receiver possess the same key. The key used to encrypt a message is also used to decrypt the encrypted message from the sender.

Asymmetric (public-key) cryptography: In this method the actual message is encoded and decoded using two different mathematically related keys, one of them is called public key and the other is called private key.

To provide the maximum security using cryptography we target the following five areas:

1. Integrity
2. Non-repudiation
3. Authenticity
4. Confidentiality
5. Privacy

Working Papers:

A Conceptual Review On E-Com Challenges (A Special Reference To Security Issues)
Members:

Vinutha H. K.

Publications:

- "Green Strategies Among The Borrowers Of Commercial Banks In Dakshina Kannada District Of Karnataka" ie International conference on **Green Banking**. ISBN NO:9789386256393.
- E-waste Management ie National Conference on **“Digital India – Prospering India”** Cancon.
- GST Implementation And Its Implication i.e Pay India National Conference on **Emerging Tax Reforms and Implications.** ISBN NO: 978-81-930542-4-6.