ACCEPTANCE

Enhancing the security and performance of Business-to-Business E-Commerce using Hybrid Model By

YISHAK SIME

Accepted by the Faculty of Informatics, St. Mary's University, in partial fulfillment of the requirements for the degree of Master of Science in Computer Science

Thesis Examination Committee:

____

Internal Examiner

____

External Examiner

____

Dean, Faculty of Informatics

February, 2022

DECLARATION

I, the undersigned, declare that this thesis work is my original work, has not been presented for a degree in this or any other universities, and all sources of materials used for the thesis work have been duly acknowledged.

____

Full Name of Student

____

Signature

Addis Ababa

Ethiopia

This thesis has been submitted for examination with my approval as advisor.

____

Full Name of Advisor

____

Signature

Addis Ababa

Ethiopia

February2, 2022

Acknowledgement

First and foremost, I thank **God** for endowing me with health, patience, and knowledge to complete this work and made me lucky to be supervised by such a **Doctor Tibebe Beshah**It gives me pleasure to thank my Advisor **Dr. Tibebe Beshah** for all he taught me, without his help, sage advice, insightful criticism, and continuous follow-up; this research would never have been.

I also want to extend my best regards to my family, my wife and to my two lovely kids for all their support and for the time they gave me on doing these thesis.

Table of Content

.

List of Figure

List of Table

Keywords: B2B, Cryptography, AES, Encryption Key, MD5

Abstract

Electronic commerce is a modern platform which allows buyer and seller to transact on line through an electronic wire without travelling long distance through crossing boundaries. It enable the sellers to penetrate the huge global market on providing goods and services to the potential buyers and initiate the buyer to purchase goods and services.

Electronic commerce cannot be realized without strong security procedure which guarantee the buyer and seller that they are transacting in safe environment which unauthorized user do not interfere their communication.

The primary essence of this thesis is to create a more reliable and efficient security environment for the electronic market in general and specifically for the Business-to-Business kind of commerce.

Various researches are made e-commerce security using the Symmetric and Asymmetric cryptographic algorithm, but only a few papers were done on reducing the execution time of algorithm without compromising the strength of security.

This thesis were done to fill the gap on reducing the execution time of the AES algorithm from 10 iteration round to 8. There were no papers done this aspect and this thesis use the standard AES algorithm and reduced the number of iteration from 10 to 8 and to avoid the limitation of AES algorithm on key exchange between the sender and receiver by decrypting the encryption key using the MD5 hashing algorithm to ensure more security.

This thesis were employed experimental research methods and measured the execution time of the standard AES algorithm and the MRRA algorithm on selected sample files of Text, PDF and Audio files of 100KB and 1MB using Java cryptoutil and the result indicates that the MRRA reduced the execution time of the standard AES algorithm by 4%.