

# **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

Acknowledgement.....	ii
Table of Contents.....	iii
List of Acronyms.....	iv
List of Figures.....	v
List of Tables.....	vi
Abstract.....	vii
<b>1. Introduction</b> .....	<b>1</b>
a. Back ground.....	1
b. Statement of the problem.....	2
c. Objectives.....	3
d. Significance of the study.....	4
e. Scope/limitation.....	4
f. Organization of the study.....	5
<b>2. Literature Review</b> .....	<b>6</b>
2.1. Introduction.....	6
2.2. Ecommerce security.....	6
2.3. Cryptographic algorithm.....	10
2.4. DES, 3DES, Blowfish and AES encryption algorithms.....	12
2.5. Message Digest 5 Algorithm.....	17
2.6. Hybrid cryptographic algorithms.....	19
<b>3. Methodology</b> .....	<b>23</b>
3.1 General approach.....	23
3.2 Specific research design.....	23
3.3 Data Collection Methods and Approaches.....	24
3.4. Experimental Process and Tools.....	24
3.4.1 Python in cryptography.....	25

3.4.2 Java Crypto Package.....	26
3.4.3 Message Digest 5 (MD5).....	26
3.5. System Architecture.....	27
3.6 AES Algorithm Description.....	28
3.6.1 Message Digest 5 (MD5) algorithm description.....	28
3.7. Validation and Evaluation Process.....	29
<b>4. Experiment and Results.....</b>	<b>30</b>
4.1. Model Description.....	30
4.2 Modified AES Algorithm Flow chart.....	32
4.3 The Four Steps in Each Round of Processing.....	33
4.4. Modified Reduced-Round AES Algorithm (MRRA).....	35
4.5. Experimental analysis.....	37
4.6. Password hashing using MD5 algorithm.....	40
4.7. Result and analysis.....	41
4.7.1. MRRA AES encryption experiment.....	43
4.7.2. MRRA AES decryption algorithm experiment.....	47
4.8. Discussion.....	55
<b>5. Conclusion and Future Works.....</b>	<b>57</b>
5.1. Conclusion.....	57
5.2 Recommendation.....	59
5.3. Future Work.....	59
<b>References.....</b>	<b>60</b>
<b>Appendix.....</b>	<b>62</b>

## List of Figure

Figure1. Dimensions of Ecommerce Security.....	7
Figure 2. Shows the different steps that are carried out in each round.....	25
Figure 3: Block diagram for Encryption and Decryption process.....	27
Figure 4. The overall structure of AES encryption/decryption.....	31
Figure 5. Modified AES Flow chart.....	32
Figure 6. MRRA Cipher Round Algorithm.....	36
Figure 7. AES encryption execution time of 100KB in millisecond.....	38
Figure 8. Standard AES execution time of size 1MB in millisecond.....	39
Figure 9. Hashing encryption key using SHA256.....	40
Figure 10. Encryption result of PDF file.....	41
Figure 11. Encryption of sample Audio file.....	42
Figure 12. Encryption of sample Text file.....	42
Figure 13. MRRA encryption File size compared with execution time.....	45
Figure 14. MRRA encryption execution time in millisecond.....	46
Figure 15. MRRA and Standard algorithm of 100KB in millisecond.....	47
Figure 16. The standard AES execution time in millisecond.....	48
Figure 17. MRRA file decryption in millisecond.....	50
Figure 18. MRRA file decryption time in millisecond.....	51
Figure 19. MRRA Encryption\ Decryption time percentage distribution.....	52
Figure 20. MRRA and Standard AES algorithm comparison.....	54

## List of Table

Table 1: Sample Test files.....	37
Table 2. Execution time for AES encryption in millisecond.....	37
Table 3: sample cipher.....	44
Table 4. MRRA encryption execution time.....	44
Table 5. Standard AES decryption algorithm execution time.....	47
Table 6. MRRA decryption execution time in millisecond.....	49
Table 7. MRRA Encryption and Decryption time in millisecond.....	52
Table 8. AES and MRRA comparison.....	53
Table 9. MRRA Encryption in different file size.....	55

**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%.