

Table of Contents

VALIDITY SHEET	i
ORIGINALITY STATEMENT SHEET	ii
DECLARATION FORM.....	iii
DEDICATION.....	iv
ABSTRACT	v
LIST OF FIGURES	ix
LIST OF TABLES	xi
LIST OF ABBREVIATIONS	xii
CHAPTER I - INTRODUCTION	1
1.1 Background	1
1.2 Problem Identification	4
1.3 Research Objective	4
1.4 Scope of Work	5
1.5 Hypotheses	5
1.6 Research Method	5
1.6.1 Technical Approach	5
1.6.2 Regulatory Approach	6
CHAPTER II - OVERVIEW OF FINTECH AND AUTHENTICATION	7
2.1 Fintech Services	7
2.2 Cyber security and Information Security	8
2.3 Authentication	9
2.3.1 Authentication Factor Classification	9
2.3.1.1 One Factor Authentication (1FA)	9
2.3.1.1 Two Factor Authentication (2FA)	9
2.3.2 Authentication Mechanism	10
2.3.2.1 Something You Know	10
2.3.2.2 Something You Have	11
2.3.2.3 Something you are	11
2.3.3 Biometric Identification	12
2.3.3.1 Fingerprint Authentication	12
2.3.3.2 Face Recognition Authentication	14

2.3.4	Feature Extraction and Classification	14
2.3.4.1	Gray-Level Co-Occurrence Matrix (GLCM)	15
2.3.4.2	K-Nearest Neighbor (KNN)	16
CHAPTER III - AUTHENTICATION REGULATIONS IN INDONESIA AND INTERNATIONAL STANDARDS		19
3.1	Regulation in Indonesia	19
3.1.1	Regulation of the Minister of Communication and Informatics	20
3.1.2	Regulation of Bank Indonesia	20
3.2	International Standardization	21
3.2.1	Payment Services Directive 2 (PSD2) and Strong Customer Authentication (SCA)	21
3.2.2	National Institute of Standards and Technology (NIST US)	23
3.2.3	Council of Europe: Convention 108	24
3.2.4	ISO/IEC 27000	25
CHAPTER IV - FRAMEWORK OF AUTHENTICATION SIMULATION AND MARKET SURVEY		28
4.1	Research Workflow	28
4.2	Modeling Simulator	29
4.3	Experimental Study	29
4.4	Biometric and Password Authentication System	30
4.4.1	Image acquisition	32
4.4.2	Preprocessing	32
4.4.3	Extraction GLCM	34
4.4.4	Classification Image	34
4.5	One Factor and Two Factor Authentication System	35
4.5.1	One Factor Authentication	35
4.5.2	Two factor Authentication	36
4.6	Simulation Scheme and Analysis	37
4.6.1	Simulation Scheme	37
4.6.2	Computation Analysis	39
4.7	Exploratory Quantitative Research	39
4.7.1	Simulation Model	40
4.7.2	Scope of Exploratory Quantitative	40
CHAPTER V - ANALYSIS OF AUTHENTICATION PERFORMANCE, MARKET SURVEY, AND REGULATION RECOMMENDATION		42
5.1	Password and Biometric Authentication Performance	42

5.1.1	Processing Time	42
5.1.2	Processing Accuracy	43
5.1.3	Processing Memory	46
5.1.4	Complexity	48
5.2	One-Factor and Two-factor Authentication Performance	49
5.2.1	Processing Time	49
5.2.2	Processing Accuracy	50
5.2.3	Processing Memory	50
5.2.4	Complexity	50
5.3	MD5 and SHA-256 Encryption Performance	50
5.3.1	Processing Time	51
5.3.2	Processing Memory	52
5.3.3	Complexity	53
5.4	Market Survey	53
5.4.1	User Profiling	54
5.4.2	User Knowledge of Data Security	56
5.4.3	User willingness for Two-factor authentication and Biometrics	57
5.5	Regulation Recommendation	59
5.5.1	Data Governance	60
5.5.2	Security and Usability	61
CHAPTER VI - CONCLUSIONS AND SUGGESTIONS		67
6.1	CONCLUSIONS AND RECOMMENDATION	67
6.2	SUGGESTIONS	68
REFERENCE		69
APPENDIX I		72
APPENDIX II		74
APPENDIX III		80
APPENDIX IV		81