

**A MODEL FOR SECURING E-EDUCATIONAL DATA FROM INSIDER  
THREATS USING BLOCKCHAIN TECHNOLOGY**

**UBAKA, MILLICENT NKIRUKA  
(15PCG01033)**

**DECEMBER, 2022**

**A MODEL FOR SECURING E-EDUCATIONAL DATA FROM INSIDER  
THREATS USING BLOCKCHAIN TECHNOLOGY**

**BY**

**UBAKA, MILLICENT NKIRUKA  
(15PCG01033)**

**B.Tech Computer Science, Federal University of Technology(FUTA), Akure  
M.Sc Computer Science, Federal University of Agriculture (FUNAAB), Abeokuta**

**A THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER AND  
INFORMATION SCIENCES IN PARTIAL FULFILMENT OF THE  
REQUIREMENTS FOR THE AWARD OF DOCTOR OF PHILOSOPHY  
(Ph.D) DEGREE IN COMPUTER SCIENCE, COLLEGE OF SCIENCE  
AND TECHNOLOGY, COVENANT UNIVERSITY, OTA, OGUN STATE,  
NIGERIA**

**DECEMBER, 2022**

## **ACCEPTANCE**

This is to attest that this thesis is accepted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science in the Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Ogun State.

**Miss. Adefunke F. Oyinloye**  
**(Secretary, School of Postgraduate Studies)**

**Signature and Date**

**Prof. Akan B. Williams**  
**(Dean School of Postgraduate Studies)**

**Signature and Date**

## **DECLARATION**

I, **UBAKA, MILLICENT NKIRUKA (15PCG01033)**, hereby declare that this research was carried out by me under the supervision of Professor Ambrose A. Azeta and Dr. Aderonke A. Oni in the Department of Computer and Information Sciences, Covenant University, Ota. I attest that the thesis has not been presented either wholly or partly for the award of any degree elsewhere. All sources of data and scholarly information used in this thesis are duly acknowledged.

**UBAKA, MILLICENT NKIRUKA**

**Signature and Date**

## **CERTIFICATION**

We certify that the thesis titled “**A MODEL FOR SECURING E-EDUCATIONAL DATA FROM INSIDER THREATS USING BLOCKCHAIN TECHNOLOGY**” is an original research work carried out by **UBAKA, MILLICENT NKIRUKA (15PCG01033)**, in the Department of Computer and Information Sciences, Covenant University, Ota, Ogun State, Nigeria, under the supervision of Professor Ambrose A. Azeta and Dr. Aderonke A. Oni. We have examined and found the work acceptable for the award of the degree of Doctor of Philosophy in Computer Science.

**Prof. Ambrose A. Azeta**  
(Supervisor)

**Signature and Date**

**Dr. Aderonke A. Oni**  
(Co-Supervisor)

**Signature and Date**

**Prof. Olufunke O. Oladipupo**  
(Head of Department)

**Signature and Date**

**Prof. Olusegun A. Ojesanmi**  
(External Examiner)

**Signature and Date**

**Prof. Akan B. Williams**  
(Dean, School of Postgraduate studies)

**Signature and Date**

## **DEDICATION**

I dedicate this research work to my Heavenly Father- The source of wisdom and in whom is no variation or shadow of turning. I also dedicate this work to my family Prince Chinedu Damian Ubaka and my children, Damian, Dominion, Daniel, and Joy Munachimso Damian-Ubaka. And to my parents, Chief & Mrs. Mike Okoye.

## ACKNOWLEDGEMENTS

I must thank GOD for providing me with a conducive learning atmosphere and the opportunity to succeed. I can see His divine hand at work in my life. God, who is both all-powerful and all-present. He is a God who is always trustworthy. In whatever situation, He is always there for me. Throughout my Ph.D studies at Covenant University, I am grateful for His kindness, mercies and wisdom. I thank the Chancellor and Chairman of the Board of Regents, Covenant University, Dr. David Oyedepo, for providing a platform that has given me the opportunity to be part of the glorious vision that Covenant University is driving. I sincerely thank the Vice-Chancellor of Covenant University, Professor Abiodun H. Adebayo, the Registrar, Dr. Oluwasegun P. Omidiora, and the entire management team for their leadership role towards the success of this program. I appreciate the Dean, School of Postgraduate Studies (SPS), Professor Akan B. Williams, and the Sub-Dean, SPS, Dr. Emmanuel O. Amoo. The Dean, College of Science and Technology, Professor Timothy A. Anake, is also appreciated.

Despite the tiresome and difficult effort needed, I am becoming increasingly conscious that research may be a pleasurable and gratifying experience at this time of my life. Professor. Ambrose A. Azeta and Dr. Aderonke A. Oni's encouragement, enthusiasm, gracious help, and lectures were crucial in the completion of this study. I have to make a note of appreciation to them. I owe them a debt of appreciation for the extensive grooming they provided me in the areas of academic, professional, and personal life; without their persistent assistance, my work would not have taken shape.

My heartfelt gratitude also goes out to all of my Covenant University lecturers for teaching and giving me the knowledge that served as the foundation for preparing this thesis.

I also like to express my gratitude to the administrative personnel in the Department of Computer and Information Sciences for their assistance and support during my academic career. Finally, I like to express my gratitude to my family, who have always believed in me and supported me no matter what.

# TABLE OF CONTENTS

<b>CONTENT</b>	<b>PAGES</b>
<b>COVER PAGE</b>	<b>i</b>
<b>TITLE PAGE</b>	<b>ii</b>
<b>ACCEPTANCE</b>	<b>iii</b>
<b>DECLARATION</b>	<b>iv</b>
<b>CERTIFICATION</b>	<b>v</b>
<b>DEDICATION</b>	<b>vi</b>
<b>ACKNOWLEDGEMENTS</b>	<b>vii</b>
<b>LIST OF TABLES</b>	<b>xii</b>
<b>LIST OF FIGURES</b>	<b>xiii</b>
<b>LIST-OF ABBREVIATIONS AND SYMBOLS</b>	<b>xv</b>
<b>ABSTRACT</b>	<b>xvii</b>
<b>CHAPTER ONE: INTRODUCTION</b>	<b>1</b>
1.1 Background to the Study	1
1.2 Statement of the Problem	3
1.3 Research Questions	4
1.4 Aim and Objectives of the Study	4
1.5 Justification for the Study	6
1.6 Scope of the Study	6
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>7</b>
2.1 Preamble	7
2.2 Securing Education Data From Insider Threats	7
2.2.1 Approaches for Insider Threats Detection	14
2.2.2 Network Model on Insider Threats	23
2.2.3 Existing Insider Threats Potential Methodologies	24
2.2.4 Shortcomings of Present Methodologies on Insider Threats	29
2.2.5 Interacting Actors with Education Data	32
2.2.6 Education Data Security Properties That Guide Users' activities	33



2.2.7	Users Activities Threats on Education Data	34
2.3	Overview of Blockchain	36
2.4	Overview of Blockchain Architecture	40
2.4.1	Blockchain Phenomenon	42
2.4.2	The 4 Ps of Blockchain	42
2.4.3	Nodes and ledger Architecture	43
2.4.4	Principles of Blockchain Security	44
2.4.5	Overview of Blocks	45
2.4.6	Transaction Mechanism in Blockchain Technology	47
2.4.7	Consensus Algorithms and Hash Algorithm Function	48
2.4.8	Blockchain Model Description	51
2.5	Categorization of Blockchain	53
2.5.1	Blockchain Use Cases	53
2.5.2	Block Chain Security Issues and Challenges	56
2.6	Value of Blockchain to Education Systems	59
2.6.1	Blockchain Effects on e-learning Credentials	60
2.6.2	Blockchain Technology Transformation of Educational Institutions	61
2.5.3	The Traditional and Blockchain Model	62
2.7	Smart Contract Modules and Their Description	63
2.8	Elliptic Curve Certificate For The Sign-Up Process	74
2.8.1	Model Design For Set-Up Process	76
2.8.2	Infected and Resistance Nodes Demonstration Model in Netlogo	76
2.9	Overview Of Concepts	77
2.9.1	Some Other Terminologies Used in Blockchain	83
2.10	Integrated Development Environment (IDE): MS Visual Studio 2019	83
2.10.1	Backend Components	85

2.11	Review of Related Works	86
2.12	Research Gap	96
	<b>CHAPTER THREE: METHODOLOGY</b>	<b>97</b>
3.1	Preamble	97
3.2	Requirement Elicitation	99
3.3	The Blockchain Model for Securing Educational Data	100
3.3.1	Description of the Blockchain Layout Sub Model for Educational Data	105
3.3.2	Model Design	107
3.3.3	Registration of Operators: Algorithm 2	108
3.3.4	The Blockchain-Based Trust Function Model	110
3.3.5	Specific Insider Threats Attack on the Network	111
3.4	Consensus Mechanism	112
3.5	Creating Decentralized Application (DApp)	118
3.5.1	Implementation of Decentralized Application	119
3.5.2	Procedure for Running the DApplications	121
3.6	Procedures and Workflow for deploying Ethereum Smart Contracts	124
3.7	Model Rules	125
3.8	Performance Analysis and Evaluation Metrics	126
3.9	Dataset	126
	<b>CHAPTER FOUR: RESULTS AND DISCUSSION</b>	<b>127</b>
4.1	Implementation Details	127
4.1.1	Security Analysis of the Implementation	129
4.2	Discussion on Scalability and Usability Evaluation of the Blockchain System with the Existing System for Evaluation	131

<b>CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS</b>	<b>139</b>
5.1 Summary	139
5.2 Conclusion	139
5.3 Contributions to Knowledge	140
5.4 Limitation of the Study	140
5.5 Recommendations	140
5.6 Research Challenges	141
<b>REFERENCES</b>	<b>142</b>
<b>APPENDIX A</b>	<b>165</b>
<b>APPENDIX B</b>	<b>167</b>
<b>APPENDIX C</b>	<b>169</b>
<b>APPENDIX D</b>	<b>170</b>
<b>APPENDIX E</b>	<b>173</b>
<b>APPENDIX F</b>	<b>174</b>
<b>APPENDIX G</b>	<b>177</b>
<b>APPENDIX H</b>	<b>180</b>
<b>APPENDIX I</b>	<b>183</b>
<b>APPENDIX J</b>	<b>184</b>
<b>APPENDIX K</b>	<b>185</b>
<b>APPENDIX L</b>	<b>188</b>
<b>APPENDIX M</b>	<b>196</b>

## **LIST OF TABLES**

<b>TABLES</b>	<b>LIST OF TABLES</b>	<b>PAGES</b>
1.1	Objectives and Methodology Mappings for the Study	5
2.1	Centralized, Decentralized and Distributed Network	44
2.2	Blockchain Security	45
2.3	Summary of Top Four (4) Blockchain	51
2.4	Configuration Containing Utilities of User Contract	66
2.5	Configuration Containing Utilities of File Contract	67
2.6	Configuration Containing Utilities of School Contract	67
2.7	Configuration Containing Utilities of Student Contract	68
2.8	Configuration Containing Utilities of File Company Contract	69
2.9	Configuration Containing Utilities of Request Contract	71
2.10	Configuration Containing Utilities of Certificate Authority Contract	71
2.11	Configuration Containing Utilities of Share File Contract	72
2.12	Configuration Containing Utilities of Fund-Raising Contract	73
2.13	Smart Contract-Related Threats and Exposure	83
2.14	Types of Insider and Relevant Threats	91
3.1	Basic Notations for System Model	102
3.2	Wei Values and the Corresponding Number of Nodes	105
3.3	Open Web Application Security Project (OWASP)	123
3.4	Free of Charge Private Ethereum Network Performance	127
4.1	Evaluation of the Blockchain System and the Existing System	133

## LIST OF FIGURES

<b>FIGURES</b>	<b>LIST OF FIGURES</b>	<b>PAGES</b>
2.1	An Overview of Blockchain Decentralized Architecture	41
2.2	Framework of Blockchain Analysis	43
2.3	Types of Networks	44
2.4	Blockchain Architecture	46
2.5	Description of Parent Block Hash	47
2.6	Process of Block-Chaining	48
2.7	Keccak Sponge Function/Construction	50
2.8	Barabasi-Albert Network	53
2.9	Blockchain(Distributed Ledger) Educational Chain	62
2.10	Certification in Blockchain	63
2.11	The Existing System Model for Educational Data Institution	64
2.12	Structure Showing Interaction Between Various Smart Contracts	74
3.1	Methodology Workflow	97
3.2	The Blockchain Model for Securing Educational Data	100
3.3	Blockchain Layout Sub Model for Educational Data	105
3.4	Consensus Mechanism Procedure	113
3.5	Procedure for Connecting with the Blockchain	114
3.6	Procedure for Creating a Transaction	116
3.7	Procedure for Generating a New Block	117
3.8	UML Class Diagram of Blockchain Model	118
4.1	Prove of Concept Using Student Result	127
4.2	Showing Ganache Application Backend	128
4.3	The Implementation of the DApp Platform Using Ethereum Blockchain	129
4.3a	Experimental Setup for Running Various Tests	130
4.4	System Users Behaviour Under Insider Threat Attack(Existing System)	132
4.5	Step Two (1)System Users Behaviour Under Insider Threat Attack (Blockchain System)	134
4.6	Setup Three (2), System Users Behaviour Under Insider Threats Attack	

	(Network Efficiency)	135
4.7	Setup four (3), System Users Behaviour Under Insider Threats Attack (Number of Transaction Processed)	136
4.8	Setup four (3), System Users Behaviour Under Insider Threats Attack (Total Block Size Processed)	137
4.9	Setup Five (5), System Users Behaviour Under Insider Threats Attack (Blockchain Cost Analysis)	138

## LIST OF ABBREVIATIONS AND SYMBOLS

<b>Acronyms</b>	<b>Full Meaning</b>
App	Application
AWS	Amazon Web Service
API	Application Programming Interface
CSS	Cascading Style Sheets
CM	Consensus Mechanism
CS	Cryptographic Signature
CGPA	Cumulative Grade Point Average
CPD	Continuing Professional Development
DApp	Decentralized Application
DAO	Distributed Autonomous Organization
DAST	Dynamic Application Security Testing
DBA	Database Administrators
DHT	Distributed Hash Table
DLT	Distributed Ledger Technology
DNS	Domain Name System
HF	Hash Functions
HMM	Hidden Markov Model
HOD	Head of Department
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IAST	Interactive Application Security Testing
ICTD	Information and Communication Technologies for Development
IDE	Integrated Development Environment
IPFS	Interplanetary File System
ISO	International Standardization Organization
JDBC	Java Database Connectivity
JSON	JavaScript Object Notation

JVM	Java Virtual Machine
LBC	Leader-Based Consensus
MIT	Massachusetts Institute of Technology
MOOC	Massively Open Online Course
NGO	Non-Governmental Organization
NOSQL	No Structured Query Language
N2N	Node to Node
PAI	Personality Assessment Inventory
POA	Proof of Authority
POS	Proof of Stake
POC	Proof of Concept
POZK	Proof of Zero Knowledge
PKI	Public key Infrastructure
PHP	Hyper Text Preprocessor
P2P	Peer to Peer
RASP	Runtime Application Self Protection
SaaS	Software as a Service
SAST	Static Application Security Testing
SDK	Software Development Kit
SUS	System Usability Scale
SQL	Structured Query Language
SVM	Support Vector Machine
TPS	Transaction Per Second
TSA	Trusted Authority
URL	Uniform Resource Locator
WAEC	West African Examination Council
WAMP	Windows Apache MySQL and PHP
XML	eXtended Markup Language



## ABSTRACT

Personnel with authorization and system administrator's privileges to the institution's secret information or Internet protocol (IP) addresses are capable of causing internal threats. There is, therefore, the need for institutions to provide a protection mechanism towards detecting insider threats occurrence route. Educational data should be upheld with the utmost integrity. Insider threats have harmed large educational institutions such as national examination boards, amongst others. Furthermore, security concerns in standardized school examinations, like insider threat, has always been a major problem that is yet to be fully addressed in educational institutions. The objective of this research is to build a model using Blockchain technology to protect e-educational data against insider threats. The methodology and techniques engaged include Blockchain Technology, Trust Function Model, Asymmetric Cryptology Model, Netlogo Model App, Ethereum, Proof of Authority Front end implementation using JavaScript, MetaMask, Microsoft Visual Studio, MongoDB, Remix, and Ganache for the backend dashboard web application. The experimental findings indicate that Blockchain system rate of recurrence of insider threat is about 30% minimum when compared with the existing model that has 70%. The developed Blockchain model can handle up to one thousand operational transactions with ease to reduce insider threats.

***Keywords: Blockchain Technology, Education Data, Data Security, Insider Threats, Online Network, Privacy, Proof of Authority (POA), Trust Model.***