UNIVERSITAS PERTAHANAN REPUBLIK INDONESIA

COMPARISON ANALYSIS BETWEEN DBN-ISOLATION FOREST AND DBN-SVM IN DETECTING CYBER ATTACKS

GILANG PRAKOSO

120220405009

A Thesis Written to Fulfill Part of the Requirements for Obtaining
a Master's Degree in Defense

FACULTY OF DEFENSE SCIENCE AND TECHNOLOGY
CYBER DEFENSE ENGINEERING

MASTER DEGREE PROGRAM
UNIVERSITAS PERTAHANAN

BOGOR
2024

UNIVERSITAS PERTAHANAN REPUBLIK INDONESIA

COMPARISON ANALYSIS BETWEEN DBN-ISOLATION FOREST AND DBN-SVM IN DETECTING CYBER ATTACKS

GILANG PRAKOSO

120220405009

A Thesis Written to Fulfill Part of the Requirements for Obtaining
a Master's Degree in Defense

FACULTY OF DEFENSE SCIENCE AND TECHNOLOGY
CYBER DEFENSE ENGINEERING

MASTER DEGREE PROGRAM
UNIVERSITAS PERTAHANAN

BOGOR

THESIS APPROVAL SHEET

Name	:	Gilang Prakoso
NIM	:	120220405009
Study Program	:	Cyber Defense Engineering
Faculty	:	Faculty of Defense Science and Technology
Thesis Title	:	Comparison Analysis Between DBN-Isolation Forest and DBN-SVM in Detecting Cyber Attacks

Supervisior I,	Supervisior II,
Dr. Ir. Aulia Khamas Heikmakhtiar, S. Kom., M.Eng Date: 26 January, 2024	Prof. Ir. Teddy Mantoro, MSc., Ph.D., SMIEEE Date: 26 January, 2024

Acknowledged by,

Dean of Faculty of Defense Science and Technology

Prof. Dr. Ir. Muhamad Asvial, M.Eng
First Class Administrator

Date: 26 Januari 2024

THESIS VALIDATION SHEET

Name	:	Gilang Prakoso
NIM	:	120220405009
Study Program	:	Cyber Defense Engineering
Faculty	:	Faculty of Defense Science and Technology
Thesis Title	:	Comparison Analysis Between DBN-Isolation Forest and DBN-SVM in Detecting Cyber Attacks

No.	Name	Signature	Date
1.	Supervisor I: Dr. Ir. Aulia Khamas Heikmakhtiar, S. Kom., M. Eng		26 January, 2024
2.	Supervisor II: Prof. Ir. Teddy Mantoro, MSc., Ph.D., SMIEEE		26 January, 2024
3.	Reviewer I: Dr. H.A. Danang Rimbawa, S.Si., M.T., C.E.H., CSBA. Colonel Navy (E) NRP 10829/P		26 January, 2024
4.	Reviewer II: Dr. Bisyron Wahyudi, S.Si., M.T.		26 January, 2024
5.	Reviewer III: Letkol Laut (KH) Dr. Hondor Saragih, S.T., M.Si(Han) 14633/P		26 January, 2024

ORIGINALITY STATEMENT

I hereby declare that in this thesis there are no works or parts of works that have been submitted to obtain a degree of any level at a university; and to the best of my knowledge there are also no terms, phrases, sentences, paragraphs, subchapters or chapters of works that have been written or published; except those that are written in this manuscript and mentioned in the List of References.

If in the future it is proven that there is plagiarism in this thesis, I am willing to accept sanctions under the provisions of the applicable laws/regulations.

Bogor, 26 Januari 2024

Gilang Prakoso

PREFACE

Praise the researcher for the presence of God Almighty, because thanks to His grace and gifts, the preparation of the thesis with the title Comparison Analysis of Deep Belief Network Combined with Isolation Forest and Support Vector Machine to Detect Cyber Attack can be completed.

This thesis is meant to fulfill one of the prerequisites for receiving a Master's degree from the Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology, University of Defense.

The research and writing of this thesis can be accomplished with the help and cooperation of numerous parties, both directly and indirectly. Therefore, on this occasion, the researcher would like to thank:

1. Mr. Major General TNI Jonni Mahroza, S.IP., MA., M.Sc., CIQnR., CIQaR., Ph.D., Chancellor of the Defense University, who provided support.
2. Dr. Ir. Aulia Khamas Heikmakhtiar, S. Kom., M. Eng. and Prof. Ir. Teddy Mantoro, MSc., Ph.D., SMIEEE as the first and second supervisors for their support and guidance during this time and for providing direction to the researcher so that this proposal and thesis can be completed.
3. The board of examiners who have provided criticism and suggestions in improving this report.
4. Colonel Laut (E) Dr. H.A. Danang Rimbawa, S.Si., M.T., M.Tr.Opsla., CEH, CSBA as the Head of the Cyber Defense Engineering Study Program and all staff, lecturers, and students at the Cyber Defense Engineering Study Program, as well as the entire Defense University community who have helped smooth the lectures.

5. Colonel Laut (P) Ruby Alamsyah, M.Tr.Opsla, M.Han, CIPA, CIT, CIIQA and Colonel Laut (E) Suginta Ginting, S.Kom, MMSI, M.Tr.Hanla. who have fully supported the thesis writing and lecture activities at the University of Defense.
6. Parties who have helped the researcher a lot during the data collection process and the writing of this thesis. Thank you for taking the time to discuss, and for sharing knowledge with researchers so that this scientific work is completed.
7. All of my beloved family, especially my mother and sister always prayed for the smooth running of the thesis.

May God Almighty reward the kindness of various parties for their help. The researcher realizes that this thesis is still imperfect, therefore with humility, the researcher hopes for constructive criticism and suggestions to support the perfection of this research.

Finally, I hope this thesis can provide benefits to the development of defense science and benefit stakeholders to improve national security and defense in the cyber field.

Bogor, 26 Januari 2024

Gilang Prakoso

ABSTRACT

COMPARISON ANALYSIS BETWEEN DBN-ISOLATION FOREST AND DBN-SVM IN DETECTING CYBER ATTACKS

GILANG PRAKOSO

This study addresses the growing attack of cyber-attacks on computer internet networks, in critical information infrastructure. The study attempts to improve detection in these networks by comparing three methods: Deep Belief Network (DBN), DBN with Isolation Forest, and DBN with Support Vector Machine. The quantitative methodology assesses the effectiveness and accuracy of various procedures in detecting abnormalities and provides numerical performance metrics. The results suggest that DBN alone is an excellent detection method for attacks, with good accuracy, precision, and recall. Furthermore, collaborative models that include DBN, Isolation Forest, and SVM show enhanced overall performance by exploiting the benefits of each method. This study has major implications for addressing security flaws and inefficiency in detection on internet networks, which is consistent with the problems raised earlier. The favorable findings of this study provide hope for the application of DBN technology, which will enable the strengthening of cybersecurity systems under legislation such as the Presidential Regulation on the Protection of Critical Information Infrastructure. The integration of DBN with other detection methods appears to be a promising strategy for improving security and contributing positively to national cyber defense.

Keywords: Cybersecurity, Deep Belief Network, Isolation Forest, Support Vector Machine, Detection.

ABSTRAK

COMPARISON ANALYSIS BETWEEN DBN-ISOLATION FOREST AND DBN-SVM IN DETECTING CYBER ATTACKS

GILANG PRAKOSO

Penelitian ini membahas ancaman cyber yang terus meningkat terhadap jaringan internet komputer, khususnya pusat data, yang menyimpan infrastruktur informasi penting. Penelitian ini mencoba untuk meningkatkan deteksi pada jaringan ini dengan membandingkan tiga metode: Deep Belief Network (DBN), DBN dengan Isolation Forest, dan DBN dengan Support Vector Machine. Metodologi kuantitatif menilai efektivitas dan akurasi berbagai prosedur dalam mendeteksi dan memberikan metrik kinerja numerik. Hasilnya menunjukkan bahwa DBN sendiri merupakan metode pendeteksian yang sangat baik untuk pusat data, dengan akurasi, presisi, dan recall yang baik. Selain itu, model kolaboratif yang mencakup DBN, Isolation Forest, dan SVM menunjukkan peningkatan kinerja secara keseluruhan dengan memanfaatkan keunggulan masing-masing metode. Penelitian ini memiliki implikasi besar untuk mengatasi kelemahan keamanan dan inefisiensi dalam deteksi di jaringan internet, yang konsisten dengan masalah yang diangkat sebelumnya. Temuan yang menguntungkan dari penelitian ini memberikan harapan untuk penerapan teknologi DBN, yang akan memungkinkan penguatan sistem keamanan siber sesuai dengan peraturan perundang-undangan seperti Peraturan Presiden tentang Perlindungan Infrastruktur Informasi Vital. Integrasi DBN dengan metode deteksi serangan lainnya tampaknya menjadi strategi yang menjanjikan untuk meningkatkan keamanan pusat data dan berkontribusi positif terhadap pertahanan siber nasional.

Kata Kunci: *Cybersecurity, Deep Belief Network, Isolation Forest, Support Vector Machine, Detection.*

TABLE OF CONTENTS

THESIS APPROVAL SHEET iii
THESIS VALIDATION SHEET iv
ORIGINALITY STATEMENT v
PREFACE vi
ABSTRACT viii
ABSTRAK ix
TABLE OF CONTENTS x
LIST OF FIGURES xiii
LIST OF TABLES xiv
LIST OF DEFINITIONS xv
CHAPTER I INTRODUCTION 1
1.1 Background 1
1.2 Problem Identification 5
1.3 Problem Limitation 5
1.4 Problem Statement 6
1.5 Research Objectives 6
1.6 Research Benefits 6
CHAPTER II LITERATURE REVIEW 8
2.1 Theoretical Foundation 8
2.1.1 National Defense 8
2.1.2 Critical Information Infrastructure (CII) 9
2.1.3 Cybersecurity 10
2.1.4 Cyber Attack 13
2.1.5 Defense Science 14
2.1.6 Deep Belief Network 14
2.1.7 Isolation Forest 16
2.1.8 Support Vector Machine 17
2.2 Previous Research 18
2.3 Thinking Framework 25

CHAPTER III RESEARCH METHODOLOGY 28
3.1 Research Method and Design 28
3.1.1 Research Method 28
3.1.2 Research Design 28
3.2 Research Place and Time 31
3.2.1 Research Place 31
3.2.2 Research Time 32
3.3 Data Collection Technique 33
3.4 Research Instruments 33
3.5 Data Process Technique 33
3.6 Data Analysis Technique 35
3.6.1 Isolation Forest 35
3.6.2 Support Vector Machine 37
3.7 Data Evaluation Technique 38
CHAPTER IV RESULTS AND DISCUSSIONS 43
4.1 Data Description 43
4.2 Data Preprocessing Results 50
4.2.1 Loading the Dataset 50
4.2.2 Convert categorical features to numerical using one-hot encoding 52
4.2.3 Label Transformation 53
4.2.4 Data Splitting 55
4.2.5 Standardization 55
4.2.6 Restricted Boltzmann Machine (RBM) Layer 56
4.2.7 Logistic Regression Layer 58
4.2.8 Build the RBM model 59
4.2.9 Train The Model 60
4.2.10 Evaluate The Model on The Test Set 61
4.2.11 Set a Threshold for Attack Detection 62
4.2.12 Isolation Forest to Detect Outliers 62
4.2.13 Support Vector Machine 63

4.3 Data Processing Results 64

4.3.1 Processing on Deep Belief Network Result 65

4.3.2 Processing on Deep Belief Network with Isolation Forest Result 68

4.3.3 Processing on Deep Belief Network with Support Vector Machine Result 69

4.4 Discussion 69

CHAPTER V CONCLUSION AND RECOMMENDATION 79

5.1 Conclusion 79

5.2 Recommendation 80

REFERENCES 82

LIST OF FIGURES

Figure 1.1 Top 10 States with the Highest Total Victim Losses in US 2
Figure 2. 1 The secure communication protocols knowledge unit topics. 12
Figure 2. 2 The Architecture of DBN. 15
Figure 2. 3 Schematic diagram of isolation tree for random partitioning six distinct unit cells. 17
Figure 2. 4 Architecture of support vector machine 18
Figure 2. 5 Research Framework. 27
Figure 3. 1 Research Design 29
Figure 4. 1 Loading the Dataset 51
Figure 4. 2. Categorical Features 52
Figure 4. 3. One-Hot Encoding 53
Figure 4. 4 Label Transformation 54
Figure 4. 5 LabelEncoder 54
Figure 4. 6 Data Splitting 55
Figure 4. 7 Standardization 56
Figure 4. 8 Restricted Boltzmann Machine (RBM) Layer 57
Figure 4. 9 RBM Linear Stack Layers 57
Figure 4. 10 Logistic Regression Layer 58
Figure 4. 11 Build the RBM model 59
Figure 4. 12 Train the Model 60
Figure 4. 13 Evaluate the Model on The Test Set 61
Figure 4. 14 Set a Threshold for Attack Detection 62
Figure 4. 15 Isolation Forest to Detect Outliers 63
Figure 4. 16 Support Vector Machine 64
Figure 4. 17 DBN Confusion Matrix 65
Figure 4. 18 DBN with Isolation Forest Confusion Matrix 68
Figure 4. 19 DBN with Support Vector Machine Confusion Matrix .. 69
Figure 4. 20 Number of Attack Forms Data on KDDCUP ‘99 70
Figure 4. 21 Model Comparisons with Deep Belief Network 72

LIST OF TABLES

Table 2. 1 Previous Research 19
Table 3. 1 Research Timeline 32
Table 3. 2 Research Tools 33
Table 3. 3 Confusion Matrix Table 40
Table 4. 1 Amount of Data in Dataset KDDCUP99……43

LIST OF DEFINITIONS

AUC	: Area Under Cover
CII	: Critical Information Infrastructure
CyBOK	: Cybersecurity Body of Knowledge
DBN	: Deep Belief Network
DDoS	: Distributed Denial of Service
DoS	: Denial of Service
FN	: False Negative
FP	: False Positive
FPR	: False Positive Rate
ICT	: Information and Comunication Technology
PERPRES	: Presidential Regulation
PUSDATIN	: Data and Information Center
R2L	: Remote to Local
RAT	: Remote Access Trojan
RBM	: Restricted Boltzmann Machine
ROC	: Receive Operating Characteristic
SVM	: Support Vector Machine
UNHAN RI	: Universitas Pertahanan Republic Indonesia
TN	: True Negative
TP	: True Positive
TPR	: True Positive Rate
U2R	: User to Root

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN RI
Terakreditasi BAN-PT "A"

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini, saya :

Nama	:	Gilang Prakoso
NIM	:	120220405009
Program StudiFakultas	:	Rekayasa Pertahanan Siber / Sains dan Teknologi Pertahanan
HP/E-mail	:	085775843444 / gilang.prakoso.gp15@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPA Perpustakaan Universitas Pertahanan Republik Indonesia, Hak Bebas Royalti *Non-Eksklusif* (*Non-exclusive Royalty-Free Right)* atas karya ilmiah yang berjudul:

" COMPARISON ANALYSIS BETWEEN DBN-ISOLATION FOREST AND DBN-SVM IN DETECTING CYBER ATTACKS"

Beserta perangkat yang diperlukan (apabila ada). Dengan Hak Bebas Royalti *Non-Eksklusif* (*Non-exclusive Royalty-Free Right)* ini UPA Perpustakaan Universitas Pertahanan Republik Indonesia berhak menyimpan, mengalih media/formatkan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencatumkan nama saya sebagai penulis/pencipta.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak UPA Perpustakaan Universitas Pertahanan Republik Indonesia, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 26 Januari 2024

Gilang Prakoso
120220405009