



Tribhuvan University
Institute of Science and Technology

**Comparison of BackPropagation Algorithm and SVM on SLA Based
Masquerader Detection in Cloud**

Dissertation

Submitted to

Central Department of Computer Science and Information Technology

Kirtipur, Kathmandu, Nepal

**In partial fulfillment of the requirements
for the Master's Degree in Computer Science and Information Technology**

by

Dadhi Ram Ghimire

February 28, 2013



Tribhuvan University
Institute of Science and Technology

**Comparison of BackPropagation Algorithm and SVM on SLA Based
Masquerader Detection in Cloud**

Dissertation

Submitted to

Central Department of Computer Science and Information Technology

Kirtipur, Kathmandu, Nepal

In partial fulfillment of the requirements

for the Master's Degree in Computer Science and Information Technology

by

Dadhi Ram Ghimire

February 28, 2013

Supervisor

Prof. Dr. Shashidhar Ram Joshi



Tribhuvan University
Institute of Science and Technology
Central Department of Computer Science and Information Technology

Student's Declaration

I hereby declare that I am the only author of this work and that no sources other than the listed here have been used in this work.

.....
Dadhi Ram Ghimire
February 28, 2013



Tribhuvan University
Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

I hereby recommend that this dissertation prepared under my supervision by Mr. Dadhi Ram Ghimire entitled “**Comparison of BackPropagation Algorithm and SVM on SLA Based Masquerader Detection in Cloud**” be accepted as partial fulfillment of the requirements for the degree of M. Sc. in Computer Science and Information Technology. In our best knowledge this is an original work in computer science.

.....

Prof. Dr. Shashidhar Ram Joshi

Institute of Engineering (IOE)

Tribhuvan University

Pulchowk, Lalitpur, Nepal

(Supervisor)



Tribhuvan University
Institute of Science and Technology

Central Department of Computer Science and Information Technology

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is satisfactory in the scope and quality as a dissertation in the partial fulfillment for the requirement of Masters Degree in Computer Science and Information Technology.

Evaluation Committee

.....
Prof. Dr. Shashidhar Ram Joshi
Institute of Engineering (IOE)
Tribhuvan University
Pulchowk, Lalitpur, Nepal
(Supervisor)

.....
Asst. Prof. Nawaraj Poudel
Head of Department (Acting HOD)
Central Department of Computer Science and
Information Technology(CDCSIT)
Tribhuvan University
Kritipur

(External Examiner)

(Internal Examiner)

ACKNOWLEDGEMENT

It is a great pleasure for me to acknowledge the contributions of a large number of individuals to this work. I deeply extend my heartily acknowledgement to my respected teacher and dissertation supervisor Prof. Dr. Shashidhar Ram Joshi, Institute of Engineering (IOE), Pulchowk, for giving me an opportunity to work under his supervision and for providing me guidance and support throughout this work.

I owe special debt of gratitude and deeply grateful to Mr. Bikash Balami (Central Department of Computer Science and Information Technology), Mr. Tej Bahadur Shahi (Central Department of Computer Science and Information Technology) and Mr. Nabin Dulal (Kathmandu engineering College) for their kind support during the study. They provided me ample time for discussion on issue related to the study and valuable suggestion in implementation portion of my dissertation.

I would like to express my gratitude to the respected teachers Prof. Dr. Subarna Shakya, Prof. Sudarshan Karanjeet, Mr. Jagdish Bhatt, Mr. Arjun Singh Saud, and others staffs of CDSCIT for granting me broad knowledge and inspirations within the time period of two years. I cannot remain without admiring the efforts put by my friends and others for their exceptional participation on this work. Last but not list, I would like to thank my family members for their constant support and encouragement.

ABSTRACT

Cloud computing is a prospering technology that most organizations are considering for adoption as a cost effective strategy for managing IT. However, organizations still consider the technology to be associated with many business risks that are yet to be resolved. Such issues include security, privacy as well as legal and regulatory risks. As an initiative to address such risks, organizations can develop and implement Service Level Agreement (SLA) to establish common expectations and goals between the cloud provider and customer. Organizations can base on the SLA to address the security concern. However, many SLAs tend to focus on cloud computing performance whilst neglecting information security issues. This study is oriented to build a masquerade detection system in cloud computing, based on the proposed SLA.

The new SLA contains additional security constraints than that found in traditional SLA such as length of temporal sequence, weight of each activities and the threshold weight of the temporal sequence.

The performance analysis includes comparison of BackPropagation algorithm with SVM. The detection rate and false alarm rate is observed and found that it can detect masqueraders well from the small set of training data with small false alarm rate.

Keywords: Cloud Computing, Service Level Agreement, Masquerader, Backpropagation Algorithm, Support Vector Machine, Temporal Sequence

TABLE OF CONTENTS

List of figures:	iv
List of Tables:	v
List of abbreviations:	vi
1. INTRODUCTION	1
1.1 Introduction.....	1
1.2 Cloud computing characteristics	1
1.3 Cloud computing services.....	2
1.3.1 Software as a Service (SaaS).....	2
1.3.2 Platforms as a Service (PaaS).....	2
1.3.3 Infrastructure as a Service (IaaS).....	3
1.4 Cloud Deployment Models	3
1.5 Motivation.....	4
1.6 Objectives	4
1.7 Organization of Thesis.....	5
2. BACKGROUND AND PROBLEM DEFINITION	6
2.1 Service Level Agreement.....	6
2.2 Security Concern	7
2.3 Masquerader.....	8
2.4 MAC Address.....	8
2.5 User Behaviour Profiling	8
2.6 Problem Definition	9
3. LITERATURE REVIEW	10
3.1 Literature Review	10
3.1.1 Information-Theoretic-based Approaches	10
3.1.2 Time based Inductive machine.....	10
3.1.3 Text Mining-based Approaches	11
3.1.4 HMM-based Approaches	11
3.1.5 Naive Bayesian based Approaches.....	11
3.1.6 SVM-based Approaches	11
3.1.7 BackPropagation Based Approach	12

3.2 Classification.....	12
3.3 Multilayer perceptrons.....	12
3.3.1 BackPropagation Algorithm.....	14
3.4 Support Vector Machine.....	15
3.4.1 Kernel Trick	16
3.4.2 Optimization.....	18
4. IMPLEMENTATION	19
4.1 Proposed SLA	19
4.1.1 Assignment of Dummy Weight.....	19
4.1.2 Length of Temporal Sequence	19
4.1.3 Selection of Threshold weight of Temporal Sequence	20
4.1.4 Device and Time Frame	20
4.2 Creation of Training and Testing Data.....	20
4.2.1 BackPropagation propagation Training and Testing Data.....	21
4.2.2 SVM Training and Testing Data	21
4.3 Classification Algorithm based on SLA Agreement	22
4.3 System Architecture for Masquerader Detection in Cloud Based on SLA	23
4.4 ANN Learning: Back Propagation Algorithm	23
4.4.1 Forward Pass: Computation of outputs of all the neurons in the network.....	23
4.4.2 Backward pass: Propagation of error and adjustment of weights	24
4.5 Considerations for choosing Network Structure	24
4.5.1 The Input Layer:	24
4.5.2 The Output Layer:	24
4.5.3 The Number of Hidden Layers:.....	25
4.6 Parameters to be considered to build BP algorithm	25
4.7 PHP.....	26
4.7 SVM Light Tool.....	26
4.8 SVM Algorithm for Training	26
4.9 SVM Algorithm for Testing.....	27
5. TESTING AND ANALYSIS	28
5.1 Backpropagation Algorithm Training and Testing	28
5.2 SVM Training and Testing	29
5.3 Evaluation Metrics	30

5.4 Experimental Results	30
6. CONCLUSION AND RECOMMENDATION	33
6.1 Conclusion	33
6.2 Future Work.....	33
REFERENCES	34
APPENDIX A	35
APPENDIX B.....	36-49

LIST OF FIGURES

Figure 1.1: A simple generalization of cloud computing system	1
Figure 1.2: Cloud computing overview model.....	4
Figure 2.1: User activity graph	9
Figure 3.1: A Multilayer Perceptron with two hidden layers	13
Figure 3.2: Support Vector Machine.....	16
Figure 3.3: Feature Mapping	17
Figure 4.1: A glimpse of Salesforce.com.....	19
Figure 4.2: System Architecture for Masquerader Detection Based on SLA	23
Figure 5.1: Sample of test data for BP Algorithm	28
Figure 5.2: Prediction made by BPNN on testing data	28
Figure 5.3: Sample of testing data for SVM.....	29
Figure 5.4: SVM learning with training data.....	29
Figure 5.5: Classifying test data with SVM	29
Figure 5.6: Column chart showing performance of SVM and BP Algorithm.....	32

LIST OF TABLES

Table 5.1: Detection rate and False alarm rate of each user.....	31
Table 5.2: Detection rate and False alarm rate of BP and SVM.....	31

LIST OF ABBREVIATIONS

SLA	Service Level Agreement
CSP	Cloud Service Provider
QoS	Quality of Service
IT	Information Technology
SVM	Support Vector Machine
ANN	Artificial Neural Network
BP	BackPropagation
BPNN	BackPropagation Neural Network
CIDD	Cloud Intrusion Detection Dataset
MLP	Multilayer Perceptron
MAC	Media Access Control
PHP	Hypertext Preprocessor
MDL	Minimum Description Length
NNID	Neural Network Intrusion Detection
TIM	Time-based Inductive Machine