



Department of information Technology

**A new Defense Mechanism Against Smishing
Attacks Using Gray Wolf Optimizer**

Prepared by

Marwan Hamid Shaker AL-Sammarraie

Supervised by

Prof. Dr. Mohamad A .Alfayomi

**This Thesis is Submitted to Faculty of Information Technology
as a Partial Fulfillment of the Requirement for Master Degree in
Software Engineering**

June 2020



Department of information Technology

**A new Defense Mechanism Against Smishing
Attacks Using Gray Wolf Optimizer**

Prepared by

Marwan Hamid Shaker AL-Sammarraie

Supervised by

Prof. Dr. Mohamad A .Alfayomi

**This Thesis is Submitted to Faculty of Information Technology
as a Partial Fulfillment of the Requirement for Master Degree in
Software Engineering**

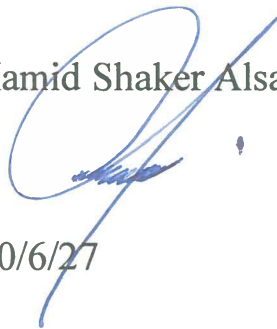
June 2020

Authorization statement

Marwan Hamid Shaker Alsammarraie authorizes Isra university to provide hard and soft copies of his thesis to libraries for the institutions or individuals upon their request

Marwan Hamid Shaker Alsammarraie

Signature



Date: 2020/6/27

اقرار تفويض

اني مروان حامد شاكر السامرائي افوض جامعة الاسراء للدراسات العليا بتزويد نسخ من رسالتي ورقياً و الكترونياً للمكتبات والمنظمات او الهيئات والمؤسسات المعنية بالابحاث والدراسات العليا عند طلبها .

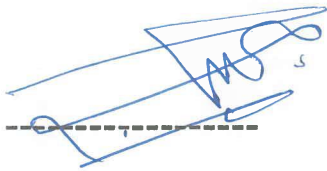
مروان حامد شاكر السامرائي

التوقيع

التاريخ : 2020/6/27

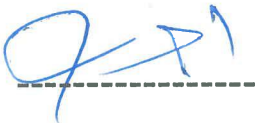


The undersigned have examined the thesis entitled **A new defense mechanism against Smishing attacks using gray wolf optimizer**, presented by **MARWAN HAMIED SHAKER ALSAMMARRAIE**, a candidate for the degree of master in software Engineering and hereby certify acceptance .



prof . Dr. Mohammad AL-Fayoumi

Date



Prof. Dr. Ahmad M. F. Al-Khasawneh

Date



Dr. Jamal Zraqo

Date

اهدي هذا العمل المتواضع :

إلى الله عز وجل خالقي ومصدر الإلهام والمعرفة

إلى من أشتاق إليه بكل جوارحي.... وطني الغالي

إلى بلدي الثاني الاردن الذي لن انسى فضله ماحييت تحت رعاية جلالة الملك المعظم
عبدالله ابن الحسين رعاه الله

إلى أبي العطوف.... قدوتي، ومثلي الأعلى في الحياة؛ فهو من علّمني كيف أعيش بكرامة
وشموخ

إلى أمي الحنوننة..... لا أجد كلمات يمكن أن تمنحها حقها، ، فهي مثال التفاني والعطاء.

إلى زوجتي.... أسمى رموز الإخلاص والوفاء ورفيقة الدرب و ملحمة الحب وفرحة العمر

إلى أولادي..... فلذات الأكباد

إلى إخوتي.... سندي وعضدي ومشاطري أفراحي وأحزاني

إلى كبار المقام اساتذتي الذين كانوا ومازالوا اخوة ناصحين محبين لم يخلوا على في علم
ولا عمل .

إلى أخي الخلق (حيدر الاعرجي) الذي علّمني أن الحياة من دون ترابط وحب وتعاون لا
تساوي شيئاً.

إلى كل من دعا لي بالخير

إلى كل من يحبني بصدق وإخلاص

إلى جموع الأقارب والأصدقاء

إن إنهنائي عملي لم يكن ليتم لولا دعمكم، وأتمنى أن ينال رضاكم.

أهديكم بحثي، وأدعو الله أن يحوز إعجابكم.

Acknowledgments

I would like to express my great gratitude to Dr. Mohamad A .Alfayomi for all his endless efforts, assistance, endless follow-up, and supervision.

Abstract

Recently, the phishing attack is one of the critical threats against Organizations, internet users, service providers, cloud computing, and many other fields in daily life. In the phishing attack, the intruder attempts to defraud the users and leak or steal the credential information, including personal information such as bank account, passwords, etc., by sending a fooled email or SMS to redirect the user to an untrusted website. Various methods have been proposed in terms of filtering and detect different types of phishing attacks; however, the researchers and security information experts are still studying to find a solution to assure the internet security from phishing and other attacks. Viewing SMS phishing messages are mostly short text and become a relatively low number associated with legitimate messages, new features for quick writing, and oversampling technique for imbalanced data utilized to SMS phishing detection. In this research, a novel framework of the SMS phishing detection presented. The proposed method combines feature extraction, oversampling, optimization algorithm for feature selection and classification. For the feature extraction and classification, the Support vector machine is implemented. In addition, the Adaptive Synthetic Sampling Approach method used to be an oversampling method. Then, the Binary Gray Wolf Optimizer Algorithm (BGWO) is applied to

analyze the extracted features and select the optimal sequence of all the features. Experimental results show that the BGWO approach enhances the accuracy of SMS phishing detection system. The proposed method in this thesis achieves the best accuracy with 99.25% by using only an average of 87.4 of features. The results demonstrate that the proposed method has a promising performance in detecting the SMS phishing messages.

List of Contents

Acknowledgments.....	vii
Chapter 1.....	1
Introduction	1
1.1 Background.....	1
1.2 Problem Statement	6
1.3 Significant of the research	8
1.4 Motivation of the Study.....	8
1.5 Research Scope and Limitations	10
1.6 Structure of the Thesis	10
Chapter 2.....	12
Attacks on SMS Messages.....	12
2.1 SMS Phishing	12
2.2 Denial of Service attack (DoS) attack	15
2.3 SMS spamming	16
2.4 SMS Phone Crashing	17
2.5 SMS Virus	18
2.6 SMS Spoofing.....	18
Chapter 3.....	20
Related Work	20
Chapter 4.....	26
Methodology.....	26
4.1 Framework for SMS phishing detection.	27
4.2 Dataset.	28
4.3 Feature detection for SMS phishing.	28
4.3.1 Token features.	29
4.3.2 Topic features	30
4.3.3 Linguistic Inquiry and Word Count Feature.....	31
4.4 Oversampling approach for imbalanced data.	32
4.5 Feature selection method based on binary GWO algorithm.	34
4.5.1 Inspiration.....	34
4.5.2 Mathematical Model	38
Chapter 5.....	43
Experiments and Results	43
Chapter 6.....	52
Conclusion and Future work.....	52
References	54

List of Figures

Figure 2.1 SMS phishing message originating from a phone number.	13
Figure 4.2 Hierarchy of grey wolf	34
Figure 4.3 The pseudo code of the GWO algorithm (Mirjalili et al., 2014).	35
Figure 4.4 Hunting behavior of grey wolves	37
Figure 4.5 The main steps of GWO algorithm.....	38
Figure 4.6 the effects of E.q. 1 and E.q. 2.....	40
Figure 4.7 3D position vectors and their possible next locations.	41
Figure 4.8 Updating the location in GWO.	42
Figure 5.1 Comparison between the proposed work and other methods.	51

List of Tables

Table 4.1 Dataset statics.....	28
Table 4.2 Initial elements of function words	30
Table 4.3 Token features	30
Table 5.4 The Expermintal results	46
Table 5.5 Classification effects of phishing SMS.	47
Table 5.6 The Experimental results for each type of feature.	48
Table 5.7 The Feature optimization result.....	49